Analiza Algorytmów, lab 3

Adrian Mucha, Politechnika Wrocławska, WPPT 12/05/2020

Zad 11

Niech $0 < q < \frac{1}{2}$ oznacza prawdopodobieństwo wydobycia kolejnego bloku przez adwersarza odpowiadające części mocy obliczeniowej będącej w jego posiadaniu.

Niech n oznacza liczbę potwierdzeń (nadbudowanych bloków) potrzebnych by uznać transakcję za potwierdzoną.

Niech $P(n, q)$ oznacza prawdopodobieństwo, że adwersarz o mocy q będzie dysponował łańcuchem bloków równym lub dłuższym niż ten budowany przez uczciwych użytkowników w momencie, gdy nadbudowali oni blok zawierający rozważaną transakcję n blokami lub kiedykolwiek później.

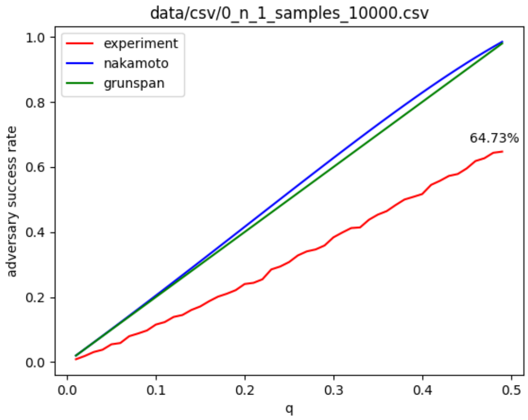
Opis symulacji ataku *„double spending"* (metoda Monte Carlo)

Pojedyncze doświadczenie polega na pobraniu 10000 próbek wydarzeń

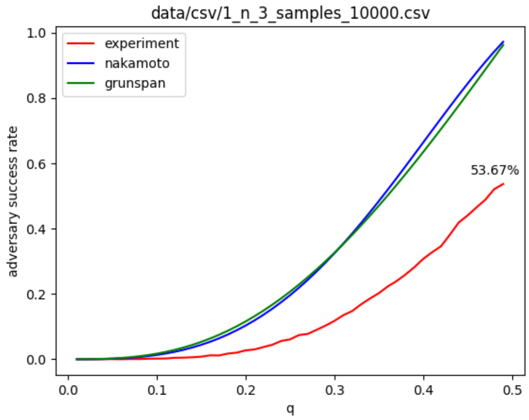
$$P(n, q) = \textit{adwersarz wygrywa atak „double spending"},$$

oraz ich uśrednieniu. Doświadczenie rozpoczyna się postawieniem zadania wykopania n bloków *dobrym użytkownikom*, którzy wykonają tę pracę w czasie $t \in (0, \infty)$. W każdej jednostce czasu *użytkownik* ma $p = 1 - q$ szans na wykopanie 1 bloku. *Adwersarz* w tym samym czasie t, kopie k bloków (ma tyle samo prób co *użytkownik*). Jeżeli $k \geq n$ to zdarzenie $P(n, q)$ uznajemy za *sukces*.

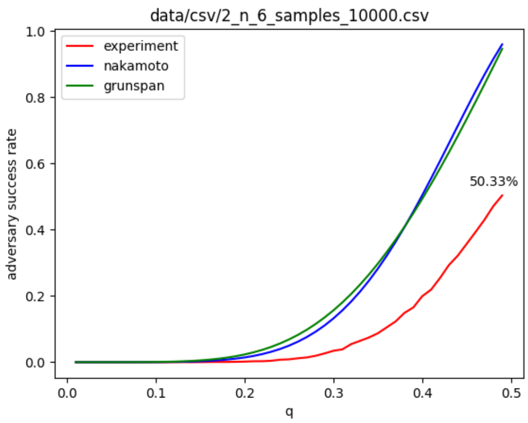
Nakamoto vs. Grunspan vs. otrzymane wyniki



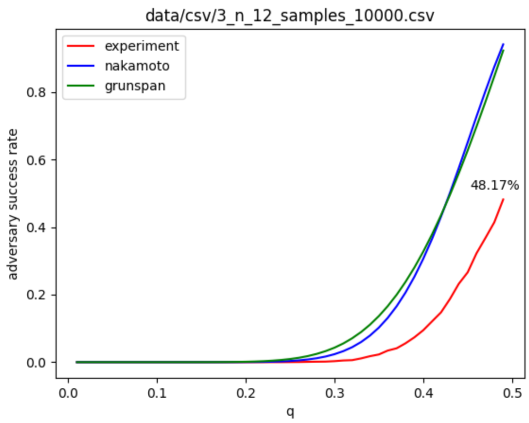
(a) $n = 1$



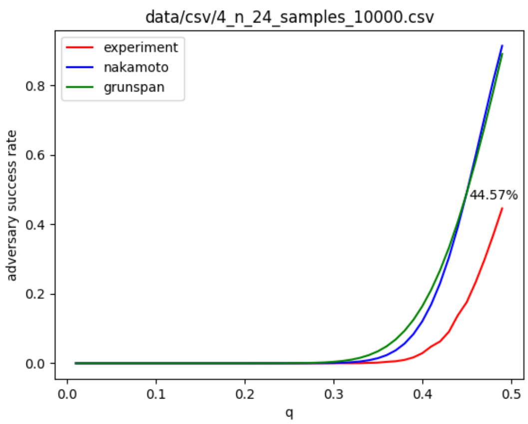
(b) $n = 3$



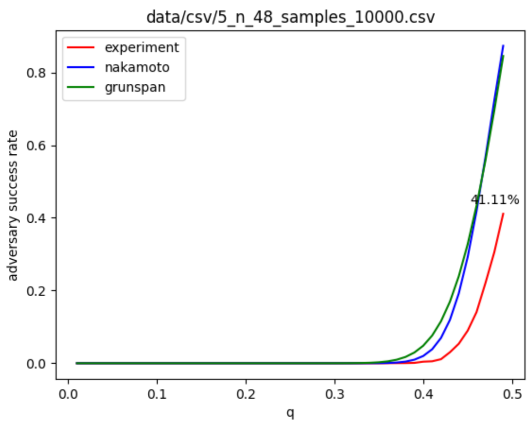
(c) $n = 6$



(d) $n = 12$



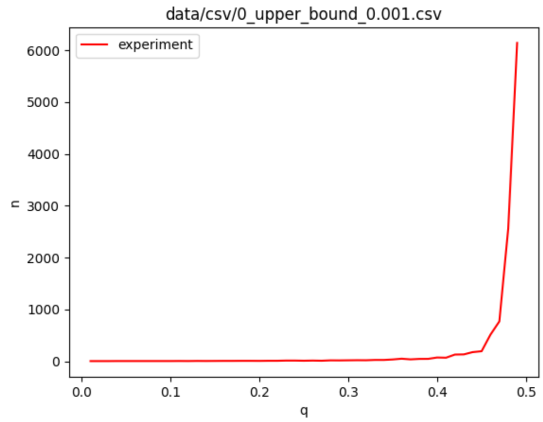
(e) $n = 24$



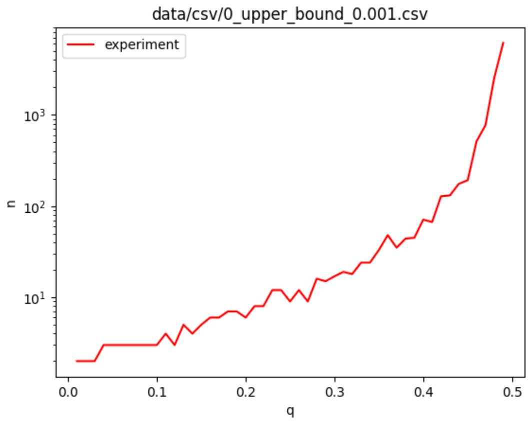
(f) $n = 48$

Figure 1: Wykresy przedstawiają prawdopodobieństwo sukcesu adwersarza w zależności od parametru q. Kolor czerwony prezentuje otrzymane wyniki gdy uruchomiono symulację 10000 razy dla każdego $0 < q < 0.5$ i uśredniono. Kolejno kolorem zielonym oraz niebieskim oznaczono formuły autorów Grunspan'a oraz Nakamoto. Jak można zauważyć, formuły narzucone przez wcześniej wspomnianych autorów są bardziej restrykcyjne. W punkcie gdy atakujący posiada niemal połowę dostępnej mocy obliczeniowej, autorzy twierdzą, że prawdopodobieństwo wygrania przez adwersarza jest prawie pewne, natomiast w danych z eksperymentu wynika iż zbliża się on jedynie do $\frac{1}{2}$ szansy na powodzenie ataku "double spending".

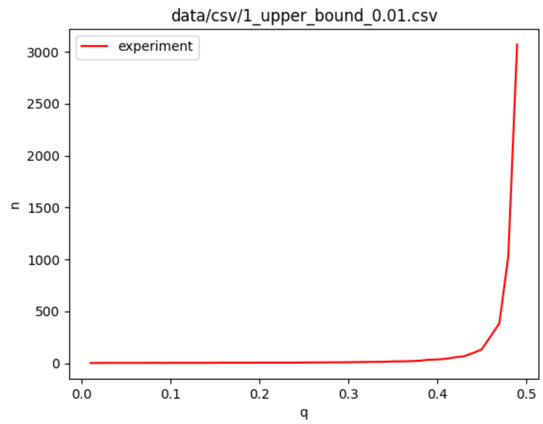
Jak dobrać n przy dopuszczalnym prawdopodobieństwie sukcesu adwersarza $P(n, q) \leq \alpha$ w zależności od q



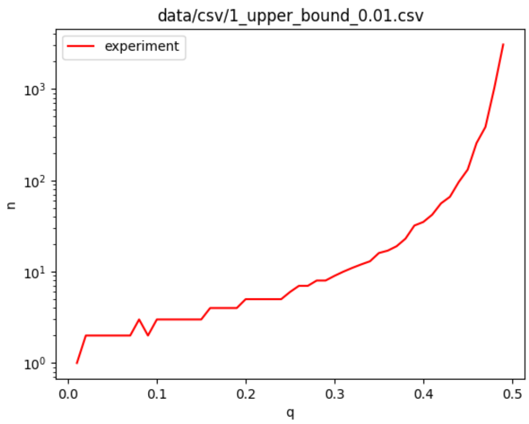
(a) $P(n, q) = 0,1\%$



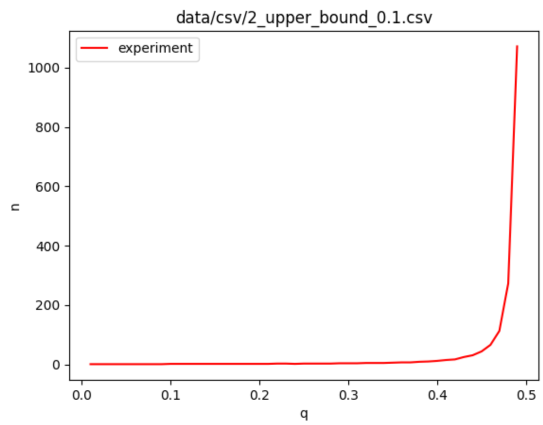
(b) $P(n, q) = 0,1\%$ (skala logarytmiczna)



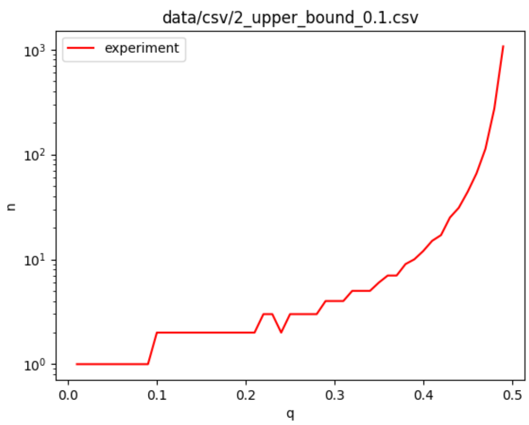
(c) $P(n, q) = 1\%$



(d) $P(n, q) = 1\%$ (skala logarytmiczna)



(e) $P(n, q) = 10\%$



(f) $P(n, q) = 10\%$ (skala logarytmiczna)

Figure 2: Można zauważyć, że gdy adwersarz dysponuje mocą bliską $\frac{1}{2}$ całej mocy obliczeniowej to wartość n drastycznie wzrasta by móc spełnić warunek dopuszczalnego prawdopodobieństwa adwersarza.