AKADEMIA GÓRNICZO-HUTNICZA

IM. STANISŁAWA STASZICA W KRAKOWIE



Wydział Inżynierii Metali i Informatyki Przemysłowej



PROJEKT ZALICZENIOWY

pt.

„Zagadnienie uzgadniania w systemach rozproszonych”

Zespół w składzie: **Krystian Cymerys**

**Konrad Boguń**

**Lucyna Hajder**

**Marcin Czanasz**

**Michał Góra**

**Karol Gałęzia**

Kierunek studiów: **Informatyka Stosowana**

Kraków 2016

Spis treści

[1. Analiza zagadnienia 4](#_Toc453081914)

[2. Algorytmy rozwiązujące zagadnienie uzgadniania 5](#_Toc453081915)

[2.1. Wybrane algorytmy 5](#_Toc453081916)

[2.2. Algorytm bizantyjskich generałów 5](#_Toc453081917)

[2.3. Algorytm randomizowany 6](#_Toc453081918)

[2.4. Algorytm jednorundowy 7](#_Toc453081919)

[2.5. Algorytm królowej 7](#_Toc453081920)

[2.6. Algorytm dwóch armii 7](#_Toc453081921)

[2.7. k-set Consensus 7](#_Toc453081922)

[2.8. Terminating Reliable Broadcast 7](#_Toc453081923)

[2.9. Algorytm tratwy 8](#_Toc453081924)

[2.10. Rozgłoszeniowy algorytm konsensusu podstawowego 8](#_Toc453081925)

[2.11. Hierarchiczny algorytm konsensusu podstawowego 8](#_Toc453081926)

[2.12. Zestawienie najważniejszych informacji o wybranych algorytmach 8](#_Toc453081927)

[Rozgłoszeniowy algorytm konsensusu podstawowego 10](#_Toc453081928)

[Hierarchiczny algorytm konsensusu podstawowego 10](#_Toc453081929)

[**3.** **Analiza porównawcza algorytmów** 11](#_Toc453081930)

[**4.** **Opis sposobu oceniania algorytmów oraz wybór najlepszego (?)** 19](#_Toc453081931)

[**5.** **Technologie rozproszone dostępne na rynku** 19](#_Toc453081932)

[**6.** **Analiza porównawcza implementacji** 19](#_Toc453081933)

[**7.** **Wnioski** 19](#_Toc453081934)

[**8.** **Bibliografia (oczywiście trzeba będzie ją poprawić)** 20](#_Toc453081935)

# Analiza zagadnienia

Problem uzgadniania, czyli innymi słowy konkretny problem osiągnięcia konsensusu, polega na tym, iż każdy węzeł w systemie rozproszonym posiada swoją wartość początkową. Następnie wszystkie węzły muszą zgodzić się na jedną z wartości określonych poprzez poszczególne pozostałe węzły. W przypadku kiedy w systemie nie dochodzi do awarii algorytm rozwiązania problemu uzgadniania jest prosty do wytłumaczenia i zrozumienia, a mianowicie: każdy z istniejących węzłów w systemie wysyła wybraną przez siebie wartość, przypuśćmy decyzję, do pozostałych węzłów. Wykonywany jest wówczas algorytm wyboru większościowego. Rezultatem takiego działania jest osiągnięcie porozumienia pomiędzy węzłami, ponieważ dysponują one takimi samymi danymi oraz wykonują ten sam algorytm, co prowadzi do zdecydowania się na tą samą wartość vel decyzję.

W niniejszym problemie istnieje możliwość wystąpienia dwóch rodzajów awarii:

* Załamania (crash failures) – awaria ta polega na tym, iż pewien węzeł przestaje wysyłać komunikaty
* Awarie bizantyjskie – polegają na tym, że istnieje jeden lub więcej wadliwy węzeł, który wysyła dowolne komunikaty

Sformułowanie problemu uzgadniania można przedstawić w sposób obrazowy, jak to jest dokonywane w większości literatury. Z tego powodu na potrzeby niniejszego projektu również skorzystano z tego sformułowania:

„Grupa armii bizantyjskich otacza miasta nieprzyjaciela. Rozkład sił jest taki, że jeśli wszystkie armie zaatakują razem, to będą w stanie zdobyć miasto. Innym sposobem uniknięcia porażki jest odwrót wszystkich armii. Generałowie poszczególnych armii mają zaufanych posłańców, którzy z powodzeniem dostarczą każdy komunikat od jednego generała do innego. Jednak niektórzy generałowie mogą być zdrajcami usiłującymi doprowadzić do porażki armii bizantyjskich. Należy opracować taki algorytm, który umożliwi wszystkim wiernym generałom uzgodnienie pewnego planu działania. Ostateczna decyzja powinna być z grubsza taka, jaka zostałby podjęta w drodze głosowania większościowego nad decyzjami poszczególnych generałów. W przypadku nierozstrzygnięcia głosowania końcową decyzją ma być odwrót.” [[[1]](#endnote-1)].

W systemie rozproszonym odpowiednikiem generałów będą węzły, natomiast posłańcy będą odpowiadać kanałom komunikacyjnym.

//MOŻNA JESZCZE COŚ DOPISAĆ

# Algorytmy rozwiązujące zagadnienie uzgadniania

W niniejszym rozdziale omówione zostaną algorytmy rozwiązujące zagadnie uzgadniania. Przedstawiono tu krótką charakterystykę każdego z wybranych algorytmów. Rozdział ten prezentuje także podstawowe informacje związane z każdym z rozwiązań, takie jak dla zgodność, skończoność czy liczba kroków dla jakich jest poprawny.

## Wybrane algorytmy

|  |  |  |  |
| --- | --- | --- | --- |
| Nazwa algorytmu | Twórca | Rok powstania | Wybrany przez |
| Algorytm generałów bizantyjskich (Byzantine Generals Algorithm) [[[2]](#endnote-2)] | Leslie Lamport  Robert Shostak  Marshall Pease | 1982 | Krystian Cymerys |
| Algorytm króla (The Phase King Algorithm) [[[3]](#endnote-3)] | Piotr Berman  Juan Garay | 1989 | Lucyna Hajder |
| Algorytm jednorundowy |  |  | Marcin Czanasz |
| Algorytm randomizowany (randomized algorithm) [[[4]](#endnote-4)] | Michael Ben-Or | 1983 | Krystian Cymerys |
| Algorytm dwóch armii (Two Army/Generals Problem) [[[5]](#endnote-5)] | Eralp Abdurrahim Akkoyunlu  Kattamuri Ekanadham  R.V. Huber | 1975 | Lucyna Hajder |
| Algorytm królowej (The Queen Algorithm) [[[6]](#endnote-6)] | Piotr Berman  Juan Garay  Kenneth Perry | 1989 | Lucyna Hajder |
| Algorytm tratwy (Raft algorithm) [[[7]](#endnote-7)] | Diego Ongaro  John Ousterhout | 2014 | Karol Gałęzia |
| Rozgłoszeniowy algorytm konsensusu podstawowego |  |  | Michał Góra |
| Hierarchiczny algorytm konsensusu podstawowego |  |  | Michał Góra |
| k-set Consensus [[[8]](#endnote-8)] | Roberto De Prisco  Dahlia Malkhi  Michael L. Reiter | 1999 | Konrad Boguń |
| Terminating Reliable Broadcast[[[9]](#endnote-9)] | Sape J. Mullender | 1993 | Konrad Boguń |

**Tabela 1.** Wybrane algorytmy rozwiązujące zagadnienie uzgadniania. Źródło: [opracowanie własne]

## Algorytm bizantyjskich generałów

Algorytm bizantyjskich generałów jest dwurundowym algorytmem rozwiązywania problemu uzgadniania. Pierwsza runda przebiega analogicznie do algorytmu jednorundowego, a mianowicie każdy z generałów, w przypadku systemu rozproszonego węzłów, podejmuje decyzję, przesyła ją do wszystkich pozostałych węzłów oraz odbiera ich decyzje. Po zakończeniu tej rundy, w tablicy przechowującej decyzję „generałów” znajdują się wszystkie decyzje, które zostały podjęte przez każdy z węzłów. Druga runda niniejszego algorytmu opiera się o założenie, iż wcześniej wspomniane decyzje zostają przesłane do pozostałych generałów. Oczywistym jest, że generał nie musi przesyłać swoich decyzji do siebie samego, a także nie musi odsyłać innemu generałowi decyzji tego generała. Analizując powyższe założenia algorytmu, można zaobserwować, iż liczba komunikatów, które generał powinien przesłać zmniejsza o jeden wraz ze wzrostem rund. Procedura głosowanie odbywa się w dwóch etapach:

* Etap I – dokonanie wyboru na podstawie decyzji otrzymanej od danego generała oznaczonego jako G oraz przekazanych informacji przez pozostałych generałów dotyczących decyzji generała G. Wynik głosowania uznaje się za „prawdziwy” i zostaje zapisany do specjalnej tablicy, która przechowuje wyniki głosowania większościowego. Procedura jest powtarzana dla każdego generała z osobna.
* Etap II – ostateczna decyzja podejmowana jest na drodze wyboru większościowego spośród wyników znajdują się we wcześniej wspomnianej tablicy, przechowującej wyniki pierwszego głosowania.

Algorytm bizantyjskich generałów może ulegać zarówno załamaniom systemu jak również awariom bizantyjskim.

## Algorytm randomizowany

Algorytm randomizowany lub inaczej zwany randomizacyjnym działa przy założeniu, że większość procesów jest prawidłowych, czyli spełnia poniższy warunek: n>2f. Łatwo zauważyć, iż powyższe wymaganie jest konieczne dla każdego algorytmu, który rozwiązuje zagadnienie konsensusu w układach asynchronicznych, jak również rozwiązania problemu uzgadniania. Wymaganie to musi być spełnione, nawet wtedy gdy wszystkie procesy mają dostęp do generatora liczb losowych.

W algorytmie randomizowanym każda wiadomość opatrzona jest specjalnym znacznikiem zawierającym etykietę (R lub P), numer rundy oraz wartość, która przyjmuje 0 lub 1. Dodatkowo wartość dla etykiety P może przyjąć stan „?”. Wiadomości oznaczone etykietą R nazywane są raportami, natomiast oznaczone etykietą P – propozycjami. Każde wykonanie pętli nazywane jest rundą i każda z nich składa się z dwóch asynchronicznych faz. W pierwszej fazie, procesy przekazują wszystkich pozostałych procesom swoją wartość decyzji (0 lub 1). W drugiej fazie, jeżeli proces otrzymał od większości raporty z tą samą wartością, to proponuje tą wartość wszystkim pozostałym procesom. W przeciwnym wypadku proponuje wartość „?”. Na koniec drugiej fazy, jeżeli proces otrzymał f+1 propozycji z tą samą wartością różną od „?”, wtedy podejmuje decyzję o ustawieniu tej wartości. W przypadku kiedy otrzyma co najmniej jedną wartość różną od „?”, to przyjmuje ją jako nowy estymat, w przeciwnym wypadku przyjmuje losową wartość swoich oszacowań [[[10]](#endnote-10)].

## Algorytm jednorundowy

Każdy generał, podejmuje decyzję, przesyła ją do wszystkich pozostałych generałów oraz odbiera ich decyzje. Ostateczna decyzja jest podejmowana na drodze wyboru większościowego spośród wszystkich decyzji, zarówno własnej jak i otrzymanych od pozostałych. Załamanie kilku generałów może spowodować niemożność uzyskania porozumienia przez pozostałych, jeśli głosy dzielą się w miarę równo.

## Algorytm królowej

## Algorytm dwóch armii

## k-set Consensus

## Terminating Reliable Broadcast

Terminating Realible Broadcast to problem występujący w systemach rozproszonych, które obudowują nadawane wiadomości w zbiór otrzymanych procesów i ich błędów. W szczególności kiedy nadawca lub inny proces może spowodować awarię w dowolnym momencie.

Protokół TRB zarządza systemem w procesie wysyłania i zbiorze procesów otrzymanych, które mogą zawierać również nadawcę. Proces nazywany jest poprawnym jeśli wystąpi awaria w trakcie jego wykonywania. Celem protokołu jest przesyłanie wiadomości od nadawcy do zestawu procesów otrzymanych. Proces może wykonywać wiele operacji I/O podczas wykonywania protokołu, ale ostatecznie dostarcza wiadomość do aplikacji na tym procesie, który wywołał protokół TRB. Wszystkie poprawne odebrane procesy muszą dostarczyć wiadomość nadawcy jeśli nadawca również był poprawny. Proces odebrany może dostarczyć specjalny komunikat – „nadawca uszkodzony”, jeżeli nadawca uległ awarii. Prawidłowy proces jest więc gwarancją, że dane dostarczone do niego są również dostarczone do pozostałych poprawnych procesów.

Protokół TRB musi spełniać poniższe własności:

• Skończoność: każdy poprawny proces wykonuję dostarcza wiadomość

• Ważność: Jeśli nadawca wiadomości m nie jest uszkodzony to wszystkie poprawne procesy dostarczają wiadomość m

• Integralność: Każdy poprawny proces dostarcza co najwyżej jedną wiadomość. Jeśli proces dostarcza wiadomość różną od null wtedy nadawca musi dostarczyć wiadomość m

• Zgodność: Jeśli poprawny proces dostarcza wiadomość m to każdy inny poprawny proces również dostarcza m.

Obecność błędów w systemie sprawia, że te właściwości są trudne do spełnienia

TRB jest ściśle powiązane z problemem konsensusu (nie jest identyczne).

## Algorytm tratwy

## Rozgłoszeniowy algorytm konsensusu podstawowego

## Hierarchiczny algorytm konsensusu podstawowego

## Zestawienie najważniejszych informacji o wybranych algorytmach

|  |  |  |  |
| --- | --- | --- | --- |
|  | Algorytm generałów bizantyjskich (The Byzantine Generals Problem) [[[11]](#endnote-11)] | Algorytm randomizowany (Randomized algorithm) [[[12]](#endnote-12)] | Algorytm jednorundowy |
| skończoność (termination) | algorytm składa się z m+1 rund w pierwszej fazie, oraz z rundy podjęcia decyzji na podstawie otrzymanych danych w drugiej fazie. Rozwiązanie gwarantuje, że wszystkie poprawne procesy w końcu podejmą decyzję dochodząc tym samym do porozumienia | algorytm składa się z stałej liczby rund. Jeżeli niektóre procesy nie mają ustawionej losowo lokalnej wartości, to ustawiają ją taką samą jak pozostałe. | algorytm składa się z jednej rundy. |
| zgodność (agreement) | wartość decyzji wszystkich poprawnych procesów jest taka sama. Jeśli p­i oraz pjsą prawidłowe oraz podjęły decyzję, wówczas di = dj | zakładając, że niektóre poprawne procesy decydują o X. Proces ten musi uzyskać X z n-3f prawidłowych procesów. Każdy inny właściwy proces musi otrzymać X co najmniej n-4f razy (wszystkie poprawne procesy ustawiają swoje lokalne wartości X, oraz proponują ją, a także decydują się na X w następnej rundzie) | załamanie kilku generałów może spowodować niemożność uzyskania porozumienia przez pozostałych, jeśli głosy dzielą się w miarę równo. |
| integralność (integrity) | jeśli dowódca jest poprawny, to wszystkie poprawne procesy decydują się na wartość decyzji, którą zaproponował dowódca | jeżeli wszystkie poprawne procesy posiadają tą samą wartość X, otrzymają n‑2f propozycji zawierających X w pierwszej rundzie oraz będą decydować o X | - |
| dla jakich kroków jest niemożliwy | poprawny tylko dla ilości procesów n>3m (zdrajców powinno być 3 razy mniej) [[[13]](#endnote-13)] | poprawny tylko dla binarnych danych wejściowych. Nie działa w przypadku kiedy istnieją procesy bizantyjskie. Działa tylko wtedy gdy istnieją f<n/9 crash failures | - |
| ilość wiadomości | n\*[(n‑1)\*n‑k)\*(n‑k‑1)] wiadomości [1] | ?? | n(n-1) wiadomości.  Każdy generał wysyła i odbiera po jednej wiadomości do i od innych generałów. |
| złożoność obliczeniowa | O(Nf+1) – dla komunikatów niepodpisanych  O(N2) – dla komunikatów podpisanych [[[14]](#endnote-14)] | O(2n) – wszystkie poprawne procesy zdecydowały  O(1/2n-f) – najgorszy przypadek, kiedy wszystkie n-f poprawnych procesów wybiera tą samą wartość losowo | O(n) |

**Tabela 2.** Podstawowe informacje o wybranych algorytmach. Źródło: [11],[12],[13],[14].

|  |  |  |  |
| --- | --- | --- | --- |
|  | Algorytm króla (Phase King Algorithm) [[[15]](#endnote-15)] | Algorytm królowej (The Queen Algorithm) [[[16]](#endnote-16)] | Algorytm dwóch armii |
| skończoność (termination) | *Algorytm zawiera 3(f + 1)* rund dla (f+1) faz.  Jeżeli król jest prawidłowy, to wszystkie prawidłowe procesy mają tą samą wartość. | *Algorytm zawiera 2(f + 1)* rund dla (f+1) faz.  Jeżeli królowa jest prawidłowa, to wszystkie prawidłowe procesy mają tą samą wartość. | Rozwiązanie może być nieskończone. Każdy proces decyduje o wartości po skończonej ilości wiadomości.[[[17]](#endnote-17)] |
| zgodność (agreement) | Wszystkie procesy mają wpływ na ostateczną wartość (króla).  Jeśli wszystkie poprawne procesy mają wartość x na początku fazy , to  nadal będą mieć x w końcowym etapie. | Wszystkie procesy mają wpływ na ostateczną wartość (królowej).  Jeśli wszystkie poprawne procesy mają wartość x na początku fazy , to  nadal będą mieć x w końcowym etapie. | Wszystkie poprawne procesy mają decydować o tej samej wartości.  Wartość jest wybrana przez proces, jeśli wystąpiła n/2 razy[[[18]](#endnote-18)] |
| integralność (integrity) | Wszystkie poprawne procesy otrzymują >= n-f odpowiedzi.  Król ustawia swoją wartość na taką, która wystąpiła więcej niż n - 2f razy i przesyła ją do wszystkich procesów. | Wszystkie poprawne procesy otrzymują >= n-f odpowiedzi.  Królowa ustawia swoją wartość na taką, która wystąpiła więcej niż n/2 + f razy i przesyła ją do wszystkich procesów. | Każdy proces otrzymuje n-f odpowiedzi. Jeśli otrzymana wartość wystąpiła >n/2 ilość, to proces zmienia wartość i przesyła ją dalej. |
| dla jakich kroków jest niemożliwy | poprawny tylko dla ilości procesorów n>3f (zdrajców powinno być 3 razy mniej) | poprawny tylko dla ilości procesorów n>4f (zdrajców powinno być 4 razy mniej) | Poprawny tylko dla ilości procesorów n > 2f |
| ilość wiadomości | (f + 1)[(n − 1)(n + 1)] wiadomości[1] | =(n-f)/2+(n-f)/2 > n/2+f wiadomości | Ilość wiadomości rośnie wykładniczo |
| złożoność obliczeniowa | O(t^3) | ??? | ??? |

**Tabela 3.** Podstawowe informacje o wybranych algorytmach cz.2. Źródło: [15],[16],[17],[18].

|  |  |  |
| --- | --- | --- |
|  | Terminating Reliable Broadcast [[[19]](#endnote-19)] | k-set Consensus [[[20]](#endnote-20)] |
| skończoność | Każdy poprawny proces dostarcza jakąś wiadomość | Każdy poprawny proces musi zdecydować się na jakąś wartość. |
| ważność | Jeśli nadawca wiadomości m nie jest uszkodzony to wszystkie poprawne procesy dostarczają wiadomość m | Jeśli jakiś proces decyduje się na jakąś wartość to musi być to wartość zaproponowana przez inny proces.  Jeden z warunków:  STRONG:  1. Decyzja dowolnego prawidłowego procesu jest równa wartości początkowej jakiego poprawnego procesu.  2. Jeśli wszystkie poprawne procesy zaczynają z wartością v to poprawne procesy decydują się na wartość v.  REGULAR:  1. Decyzja dowolnego prawidłowego procesu jest równa wartości początkowej jakiego procesu.  2.Jeśli wszystkie procesy zaczynają z wartością v to poprawne procesy decydują się na wartość v.  WEAK:  1.Jeśli nie wystąpiły błędy to decyzja dowolnego procesu jest równa wartości początkowej jakiegoś procesu.  2.Jeśli nie wystąpiły błędy i wszystkie procesy zaczęły z wartością v to każdy proces decyduje się na wartość v.  tl;dr Jeśli jakiś proces decyduje się na jakąś wartość to musi być to wartość zaproponowana przez inny proces. |
| integralność | Każdy poprawny proces dostarcza co najwyżej jedną wiadomość. Jeśli proces dostarcza wiadomość różną od null wtedy nadawca musi dostarczyć wiadomość m. |  |
| zgodność | Jeśli poprawny proces dostarcza wiadomość m to każdy inny poprawny proces rówież dostarcza m. | Wszystkie poprawne procesy muszą podjąć decyzję. Zbiór wartości na które procesy mogą się zdecydować wynosi co najwyżej k (>f) wartości. |
| złożoność obliczeniowa | D+ƒd | ? |
| dla jakich kroków jest poprawny | Poprawny proces zawsze otrzymuje wiadomość nawet jeżeli wystąpi błąd podczas wysyłania wiadomości (w tym przypadku proces dostaje wiadomość null). |  |

Tabela 4. Podstawowe informacje o wybranych algorytmach cz.3. Źródło: [19],[20].

|  |  |  |
| --- | --- | --- |
|  | Rozgłoszeniowy algorytm konsensusu podstawowego | Hierarchiczny algorytm konsensusu podstawowego |
| skończoność (termination) | Algorytm składa się z n+1 rund, a każda wiadomość jest oznaczona numerem rundy.  Wszystkie poprawne procesy ostatecznie decydują się na jakąś wartość. W systemie asynchronicznym, czas podejmowania decyzji jest przy tym skończony, ale nieznany.  Procesy wspólnie uzgadniają podejmowane decyzje, by ostatecznie zdecydowały się na jedną wartość. | Algorytm składa się z n+1 rund, a  każdy proces pełni rolę lidera rundy.  Procesy wspólnie uzgadniają podejmowane decyzje, by ostatecznie zdecydowały się na jedną wartość. |
| zgodność (agreement) | Wymaga się, by wszystkie procesy decydowały się na tę samą wartość.  Jeżeli żaden proces nie ulega awarii, procesy podejmują decyzję w pierwszej rundzie.  Nie istnieją dwa poprawne procesy, które zdecydowały się na inne wartości. Tym samym, poprawne procesy uzgadniają wspólną wartość.  W przypadku, w którym kolejno ulegają awarii wszystkie procesy, algorytm wymaga *n* rund. | Wymaga się, by wszystkie procesy decydowały się na tę samą wartość.  Lider rundy rozgłasza swoją decyzję, która jest przejmowana przez pozostałe procesy, po czym zaczyna się kolejna runda z nowym liderem.  Jeżeli lider ulegnie awarii, jego rolę przejmuje kolejny proces. |
| integralność (integrity) | Algorytm stosuje mechanizm podstawowego rozgłaszania niezawodnego oraz mechanizm doskonałego detektora awarii  Każdy proces decyduje się tylko raz. Procesy nie mogą zatem zmieniać raz podjętych decyzji.  Do podjęcia decyzji używana jest dowolna deterministyczna funkcja, znana wszystkim procesom. Na przykład wybierana może być najmniejsza wartość spośród zaproponowanych. | Algorytm stosuje mechanizm podstawowego rozgłaszania niezawodnego oraz mechanizm doskonałego detektora awarii  Hierarchia procesów jest zdefiniowana przez uporządkowanie procesów według indeksów. |
| dla jakich kroków jest niemożliwy | Algorytm przeznaczony jest dla modelu jawnych awarii. | Algorytm przeznaczony jest dla modelu jawnych awarii. |
| ilość wiadomości | Przypadek optymistyczny:  Przypadek pesymistyczny:  ) | Przypadek optymistyczny:  Przypadek pesymistyczny: |
| Złożoność obliczeniowa | Przypadek optymistyczny  Złożoność czasowa wynosi 1  Przypadek pesymistyczny  złożoność czasowa wynosi *n* | Przypadek optymistyczny  Złożoność czasowa wynosi 1  Przypadek pesymistyczny  złożoność czasowa wynosi *n* |

**Tabela 5.** Podstawowe informacje o wybranych algorytmach cz.4. Źródło: [dopisać]

//MICHAŁ, który link tyczy się którego algorytmu

<https://books.google.pl/books?id=PvJpCQAAQBAJ&pg=PA357&lpg=PA357&dq=Broadcast+algorithm+basic+consensus&source=bl&ots=znKOs_bY52&sig=7SOrkqUtE_N91bpb75NpeVzUE2Y&hl=pl&sa=X&ved=0ahUKEwj6yLyMz_fMAhXpFJoKHTn4AKkQ6AEIPDAD#v=onepage&q=Broadcast%20algorithm%20basic%20consensus&f=false>

*Projektowanie systemów mikroprocesorowych,* autor: Paweł Hadam, wyd: BTC

# Analiza porównawcza algorytmów

złożoności obliczeniowej

|  |  |  |
| --- | --- | --- |
| Algorytmy uzgadniania | Złożoność obliczeniowa | |
| Optymistyczna | Pesymistyczna |
| Algorytm bizantyjskich Generałów | O(Nf+1) | O(N2) |
| Randomized algorithm | O(2n) | O(1/2n-f) |
| Algorytm króla | O(t3) | ??? |
| Algorytm królowej | O(t3) | ??? |
| Algorytm dwóch armii | ??? | ??? |
| Terminating Reliable Broadcast | D+ƒd | ??? |
| K-set Consensus | ??? | ??? |
| Algorytm jednorundowy | O(n) | ??? |
| Rozgłoszeniowy algorytm konsensusu podstawowego | O(1) | O(n) |
| Hierarchiczny algorytm konsensusu podstawowego | O(1) | O(n) |
| Algorytm tratwy (raft consensus algorithm) | ??? | ??? |

f - ilość rund komunikacji

N - ilość komunikatów

D -

Złożoność czasowa:

|  |  |
| --- | --- |
| Algorytmy uzgadniania | Zakres stosowalności |
| Algorytm bizantyjskich Generałów | Wartość decyzji wszystkich poprawnych procesów jest taka sama. Jeśli p­i oraz pj są prawidłowe oraz podjęły decyzję, wówczas di = dj. Poprawny tylko dla ilości procesów n>3m (zdrajców powinno być 3 razy mniej) |
| Randomized algorithm | Procesy decydują o X, a jeden z nich musi uzyskać X z n-3f prawidłowych procesów. Każdy inny właściwy proces musi otrzymać X co najmniej n-4f razy, poprawny tylko dla binarnych danych wejściowych. Nie działa w przypadku kiedy istnieją procesy bizantyjskie. Działa tylko wtedy gdy istnieją f<n/9 crash failures. |
| Algorytm króla | Jeśli wszystkie poprawne procesy mają wartość X na początku fazy , to będą ją mieć w końcowym etapie. Poprawny tylko dla ilości procesorów n>3f (zdrajców powinno być 3 razy mniej) |
| Algorytm królowej | Jeśli wszystkie poprawne procesy mają wartość X na początku fazy, to będą ją mieć w końcowym etapie. Poprawny tylko dla ilości procesorów n>4f (zdrajców powinno być 4 razy mniej) |
| Algorytm dwóch armii | Poprawne procesy mają decydować o tej samej wartości. Wartość jest wybrana przez proces, jeśli wystąpiła n/2 razy. Poprawny tylko dla ilości procesorów n > 2f. |
| Terminating Reliable Broadcast | Jeśli nadawca wiadomości m nie jest uszkodzony to wszystkie poprawne procesy dostarczają wiadomość m. Poprawny proces zawsze otrzymuje wiadomość nawet jeżeli wystąpi błąd podczas wysyłania wiadomości (w tym przypadku proces dostaje wiadomość null). |
| K-set Consensus | Jeśli jakiś proces decyduje się na jakąś wartość to musi być to wartość zaproponowana przez inny proces. Wszystkie poprawne procesy muszą podjąć decyzję.  Zbiór wartości na które procesy mogą się zdecydować wynosi co najwyżej k (>f) wartości. |
| Algorytm jednorundowy | Załamanie kilku generałów może spowodować niemożność uzyskania porozumienia przez pozostałych, jeśli głosy dzielą się w miarę równo. n(n-1) wiadomości.  Każdy generał wysyła i odbiera po jednej wiadomości do i od innych generałów. |
| Rozgłoszeniowy algorytm konsensusu podstawowego | Jeżeli żaden proces nie ulega awarii, procesy podejmują decyzję w pierwszej rundzie.  W przypadku, w którym kolejno ulegają awarii wszystkie procesy, algorytm wymaga *n* rund. |
| [Hierarchiczny algorytm konsensusu podstawowego](http://wazniak.mimuw.edu.pl/index.php?title=Pr-1st-1.1-m13-Slajd25) | Lider rundy rozgłasza swoją decyzję, która jest przejmowana przez pozostałe procesy, po czym zaczyna się kolejna runda z nowym liderem. Jeżeli lider ulegnie awarii, jego rolę przejmuje kolejny proces. |
| Algorytm tratwy (raft consensus algorithm) | Lider wybierany jest głosem większości. Lider akceptuje wpisy w logu, rozsyła je na inne serwery i mówi im że mogą zaaplikować zmiany w swoich maszynach stanu. |

trudności implementacyjne

|  |  |
| --- | --- |
| Algorytmy uzgadniania | Zakres stosowalności |
| Algorytm bizantyjskich Generałów | p1: decyzja[mójID] <- wybierzAtakLubOdrót  p2: dla każdego innego generała G  p3: send(G, mójID, decyzja[mójID])  p4: dla każdego innego generała G  p5: receive(G, decyzja[G])  p6: dla każdego innego generała G  p7: dla każdego innego generała G’ z wyjątkiem G  p8: send(G’, mójID, decyzja[mójID])  p9: dla każdego innego generała G  p10: dla każdego innego generała G’ z wyjątkiem G  p11: receive(G, G’, przekazywanaDecyzja[G, G’])  p12: dla każdego innego generała G  p14: wybórWiększościowy[mójID] <- decyzja[mójID]  p15: ostatecznaDecyzja <- większość(wybórWiększościowy) |
| Randomized algorithm | p1: x:=own input; r = 0  p2: Broadcast proposal(x, r)  p3: In each round r =1,2,…  p4: Wait for n-f proposals  p5: If at least n-­2f proposals have some value y  p6: x := y; decide on y  p7: else if at least n-­4f proposals have some value y  p8: x := y;  else  p9: choose x randomly with P[x=0] = P[x=1] = ½  p10: Broadcast proposal(x, r)  p11: If decided on a value -> stop |
| Algorytm króla | p1: decyzja[mójID] <- wybierzAtakLubOdwrót  p2: wykonaj dwa razy  p3: dla każdego innego generała G  p4: send(G, mójID, decyzja[mójID])  p5: dla każdego innego generała G  p6: receive(D, decyzja[G])  p7: mojaWiększość <- większość(decyzja)  p8: większośćGłosów <- liczba głosów za decyzją mojaWiększość  p9: if ma być teraz królem  p10: dla każdego innego generała G  p11: send(G, mójID, mojaWiększość)  p12: decyzja[mójID] <- mojaWiększość  else  p13: receive(IDkróla, decyzjaKróla)  p14: if większośćGłosów > 3  p15: decyzja[mójID] <- mojaWiększość  else  p16: decyzja[mójID] <- decyzjaKróla  p17: ostatecznaDecyzja <- decyzja[mójID] |
| Algorytm królowej | p1: In each phase i ϵ 1...f+1:  Round 1:  p2: Broadcast own value  p3: Set own value to the value that was received most often  p4: If own value appears > n/2+f times  p5: support this value  else  p6: do not support any value  Round 2:  p7: The queen broadcasts its value  p8: If not supporting any value  p9: set own value to the queen’s value |
| Algorytm dwóch armii | p1: Initially Vi = {xi}  p2: for k = 1 to f+1 do  p3: send { v ∈ Vi : pi has not already send v} to all  p4: receive Vj from pj for all j (including i)  p5: Vi = U (n-1, j=0) Vj  p6: yi = min(Vi) |
| Terminating Reliable Broadcast | sender s in round 0:  p1: extract m  sender in round 1:  p2: send < m, sig( s ) > to all  Process p in round k, 1 <= k <= f+1  p3: if p extracted m from a valid message < m, sig(p1), … ,sig(pk-1) > in round k-1 and p≠sender then  p4: send <m,sig ( p1), ..., sig (pk-1), sig( p ) > to all  p5: receive round k messages from all processes  p6: for each valid round k message < m, sig ( p1), ..., sig(pk-1), sig (pk)> received by p  p7: if p has not previously extracted m then  p8: extract m  p9: if k = f + 1 then  p10: if in theentire execution p has extracted exactly one m then  p11: deliver( m )  p12: else deliver (SF)  p13: halt  http://www.cs.utexas.edu/~lorenzo/corsi/cs380d/past/03F/notes/10-30.pdf |
| K-set Consensus | p1: A process Pi, 1 < i < n, initiates k-set consensus:  p2: updatei (Obj[i]) with v;  p3: repeat  p4: local, array <- scan (Obj);  p5: until there are at least |N| - f non-null values in Obj;  p6: v <- max. of the values in local array  https://www.cs.uic.edu/~ajayk/Chapter14.pdf |
| Algorytm jednorundowy | p1: decyzja[mojID] <- wybierzAtakLubOdwrót  p2: dla każdego innego generała G  p3: send (G, mójID, decyzja[mójID])  p4: dla każdego innego generała G  p5: receive(D, decyzjap[G])  p6: ostatecznaDecyzja <- większość(decyzja) |
| Rozgłoszeniowy algorytm konsensusu podstawowego | p1: when e\_proposerRC( Pi, vi ) do  p2: proposalSeti = { vi }  p3: propOut.roundNO = roundNoi  p4: propOut.proposedValue = proposalSeti  p5: sendBRB (Qi, propOut)  p6: end when  p7: when e\_crash( P ) do  p8: correcti = correcti \ { Pj }  p9: end when  p10: when e\_receiveBRB (Qj, Qi, mS : MYPROP) do  p11: proposalSeti = proposalSeti ᑌ mS.proposedValue  p12: correctThisRoundi = correctThisRound ᑌ { Pj }  p13: end when  p14: when (correct ᑕ correctThisRoundi) ᐱ (decidedi = nil) do  p15: if correctThisRoundi = correctLastRoundi then  p16: decidedi = MIN( proposalSeti )  p17: decideRC ( Pi, decidedi )  p18: decOut.roundNo = roundNoi  p19: decOut.decidedValue = decidedi  p20: sendBRB ( Qi, decOut )  p21: else  p22: roundNoi = roundNoi + 1  p23: correctLastRoiundi = correctThisRoundi  p24: correctThisRoundi = Ø  p25: propOut.proposedValue = proposalSeti  p26: propOut.roundNo = roundNoi  p27: send (Qi, propOut)  p28: end if  p29: end when  p30: when e\_receiveBRB (Qj, Qi, dIn: DECIDED) do  p31: if decidedi = nil then  p32: decidedi = dIn.decidedValue  p33: decideRC (Pi, decidedi)  p34: decOut.roundNo = roundNoi + 1  p35: decOut.decidedValue = decidedi  p36: sendBRB (Qi, decOut)  p37: fi  p38: end when  http://wazniak.mimuw.edu.pl/index.php?title=Pr-1st-1.1-m13-toc |
| [Hierarchiczny algorytm konsensusu podstawowego](http://wazniak.mimuw.edu.pl/index.php?title=Pr-1st-1.1-m13-Slajd25) | p1: when e\_proposerRC( Pi, vi ) do  p2: proposalSeti = { vi }  p3: end when  p4: when e\_crash( P ) do  p5: suscpectedi = suspectedi ᑌ { Pj }  p6: end when  p7: when liderSeti [RoundNoi] = Pi ᐱ proposali != nil ᐱ broadcast [roundNoi] = False do  p8: decideRC ( Pi, proposali )  p9: broadcast [roundNoi] = True  p10: decOut.decideValue = proposali  p11: decOut.roundNo = roundNoi  p12: sendBRB ( Qi, decOut )  p13: end when  p14: when liderSeti [roundNo] suscpectedi ᐯ delivered [roundNo] = True do  p15: roundNoi = roundNoi + 1  p16: end when  p17: when e\_receive (Qj, Qi, dIn : DECIDED) do  p18: if (i > dIn.roundNo > propRoundNoi) then  p19: proposali = dIn.decidedValue  p20: propRoundNoi = dIn.roundNo  p21: end if  p22: k = dIn.roundNo  p21: deliveredi[k] = True  p22: end when |
| Algorytm tratwy (raft consensus algorithm) | ᑕ ᑌ ᐱ Ø ᐯ ∈ |

znanych realizacji/wdrożeń

|  |  |
| --- | --- |
| Algorytmy uzgadniania | Znane realizacje wdrożenia |
| Algorytm bizantyjskich Generałów  Algorytm Króla  Algorytm Królowej  Algorytm Dwóch Armii  Algorytm jednorundowy | * I[nterne](https://pl.wikipedia.org/wiki/Internet)t – błędy przekazywania pakietów w sieci wymusiły powstanie protokołu [TCP](https://pl.wikipedia.org/wiki/TCP_%28protok%C3%B3%C5%82%29), który zapewnia uzgodnienie wiedzy drugiego rzędu * K[ryptografi](https://pl.wikipedia.org/wiki/Kryptologia)a – zagadnienia zbliżone do [autoryzacji](https://pl.wikipedia.org/wiki/Autoryzacja_%28informatyka%29) stron * E[lektroni](https://pl.wikipedia.org/wiki/Elektronika)ka – zagadnienia przekazywania danych w warunkach wysokich zakłóceń, uzgadnianie wspólnych parametrów transmisji * S[ystemy wieloagentow](https://pl.wikipedia.org/wiki/System_wieloagentowy)e – uzgadnianie wiedzy agentów * T[eoria gier](https://pl.wikipedia.org/wiki/Teoria_gier) – zagadnienia współpracy między kilkoma graczami |
| Randomized algorithm | * W sieci reakcji chemicznych (ang. [chemical reaction network](https://en.wikipedia.org/wiki/Chemical_reaction_network)) * Objętość wypukłego ciała może być wyestymowana przez losowy algorytm z określoną precyzją w czasie wielomianowym * W złożoności komunikacji, równość dwóch stringów może zostać sprawdzona używając bitów komunikacji wraz z losowym protokołem |
| Przerywanie niezawodnego rozgłaszania  Terminating Reliable Broadcast | Brak **znanych** realizacji/wdrożeń.  https://www1.cs.fau.de/filepool/teaching/dependablesystems-2007/PDS\_20070510.pdf |
| K-set Consensus  Rozgłoszeniowy algorytm konsensusu podstawowego  [Hierarchiczny algorytm konsensusu podstawowego](http://wazniak.mimuw.edu.pl/index.php?title=Pr-1st-1.1-m13-Slajd25) | * Synchronizacja zegara (ang. [clock synchronization](https://en.wikipedia.org/wiki/Clock_synchronization)) * PageRank * Kontrola UAV (ang. [control of UAVs](https://en.wikipedia.org/wiki/Unmanned_aerial_vehicle)) * Równoważenie obciążeń (ang. [load balancing](https://en.wikipedia.org/wiki/Load_balancing_%28computing%29) ) |
| Algorytm tratwy (raft consensus algorithm) | Systemy które implementują algorytm tratwy:   * Chubby * ZooKeeper * Spanner   Chubby i Spanner nie zostały opublikowane w szczegółach, choć twórcy obu twierdzą, że bazują na Paxos. Algorytm ZooKeeper został opublikowany w szczegółach, ale jest różny od Paxos.  -VIewstamped Replication Oki i Liskova - alternatywne podejście do problemu uzgadniania, stworzone mniej więcej wtedy co Paxos. VR korzysta z podejścia opartego na liderach, z wieloma podobieństwami do Raft.  Źródła:  http://ramcloud.stanford.edu/raft.pdf  -Systems that implement consensus algorithms, such as Chubby [2, 4], ZooKeeper [11, 12], and Spanner [6]. The algorithms for Chubby and Spanner have not been published in detail, though both claim to be based on Paxos. ZooKeeper’s algorithm has been published in more detail, but it is quite different from Paxos.  -Oki and Liskov’s Viewstamped Replication (VR), an alternative approach to consensus developed around the same time as Paxos. The original description [29] was intertwined with a protocol for distributed transactions, but the core consensus protocol has been separated in a recent update [22]. VR uses a leaderbased approach with many similarities to Raft. |

|  |  |  |  |
| --- | --- | --- | --- |
| Nazwa algorytmu | popularność (ilość wyników w google | pseudokod (ilość linijek) | znane realizacje/wdrożenia |
| algorytm bizantyjskich generałów | 265 000 | 15 | 5 |
| randomized algorithm | 176000 | 11 | 3 |
| algorytm dwóch armii | 237 000 | 6 | 5 |
| algorytm króla | 2630 | 17 | 5 |
| algorytm królowej | 4200 | 9 | 5 |
| terminating reliable broadcast | 981 | 13 | 0 |
| k-set consensus | 2470 | 6 | 4 |
| algorytm jednorundowy | 2 | 6 | 5 |
| rozgłoszeniowy algorytm konsensusu podstawowego | 90 | 38 | 4 |
| [Hierarchiczny algorytm konsensusu podstawowego](http://wazniak.mimuw.edu.pl/index.php?title=Pr-1st-1.1-m13-Slajd25) | 3 | 22 | 4 |
| raft algorithm | 2070 |  | 3 |

# Opis sposobu oceniania algorytmów oraz wybór najlepszego (?)

# Technologie rozproszone dostępne na rynku

W poniższym rozdziale przedstawione zostaną aktualne technologie rozproszone, które są dostępne na rynku informatycznym. Wyniki badania rynkowego zostaną przedstawione w formie tabeli z podstawowymi informacjami.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Technologia | Firma odpowiedzialna | Aktualna wersja | Podstawowe informacje | Data powstania | Języki programowania |
| Gniazda (sockety) |  |  |  |  |  |
| RPC |  |  |  |  |  |
| RMI |  |  |  |  |  |
| webServices |  |  |  |  |  |
| CORBA |  |  |  |  |  |
| SOAP |  |  |  |  |  |
| XML |  |  |  |  |  |
| WSDL |  |  |  |  |  |
| Python |  |  |  |  |  |
| Systemy gridowe |  |  |  |  |  |

## Analiza porównawcza implementacji

## Wnioski

# **Bibliografia (oczywiście trzeba będzie ją poprawić)**

1. Ben-Ari M., „Podstawy programowania współbieżnego i rozproszonego, wyd. 2 zm. i rozsz.”, rozdział 12, str. 237-240, Wydawnictwa Naukowo-Techniczne, 2009, Warszawa [↑](#endnote-ref-1)
2. The Byzantine Generals Problem (with Marshall Pease and Robert Shostak), ACM Transactions on Programming Languages and Systems 4, 3 July 1982, <http://research.microsoft.com/users/lamport/pubs/byz.pdf>, (dostęp: 22.05.2016) [↑](#endnote-ref-2)
3. Berman P., Garay J A., Perry K.J., “Towards Optimal Distributed Consensus”, 30th IEEE Annual Symposium on Foundations of Computer Science (FOCS), str. 410-415, IEEE, ISBN: 0‑8186-1982-1, <http://zoo.cs.yale.edu/classes/cs426/2013/bib/berman89towards.pdf>, (dostęp: 03.06.2016r.) [↑](#endnote-ref-3)
4. Ben-Or M., “Another advantage of free choice: completely asynchronous agreement protocols”, PODC ’83 Proceedings of the second annual ACM symposium on Principles of distributed computing, str.27-30, ACM New York, ISBN: 0-89791-110-5, <http://dl.acm.org/citation.cfm?id=806707>, (dostęp: 03.06.2016r.) [↑](#endnote-ref-4)
5. Akkaoyunlu E.A., Ekanadham K., Huber R.V., “Some constraints and tradeoffs in the design of network communucations”, SOSP ’75 Proceedings of the fifth ACM symposium on Operating system principles, str. 67-74, ACM New York, DOI: 10.1145/800213.806523, <http://hydra.infosys.tuwien.ac.at/teaching/courses/AdvancedDistributedSystems/download/1975_Akkoyunlu,%20Ekanadham,%20Huber_Some%20constraints%20and%20tradeoffs%20in%20the%20design%20of%20network%20communications.pdf>, (dostęp: 03.06.2016r.) [↑](#endnote-ref-5)
6. Berman P., Garay J.A., Perry K.J., “Optimal early stopping in distributed consensus”, 6th International Workshop, WDAG ’92, Haifa, Israel, Springer Berlin Heidelberg, ISBN: 978-3-540-56188-0, <http://link.springer.com/chapter/10.1007/3-540-56188-9_15>, (dostęp: 03.06.2016r.) [↑](#endnote-ref-6)
7. Ongaro D., Ousterhout J., “In Search of an Understandable Consensus Algorithm”, Proc ATC’14 USENIX Annual Technical Conference, USENIX, <https://raft.github.io/raft.pdf>, (dostęp: 03.06.2016r.) [↑](#endnote-ref-7)
8. De Prisco R., Malkhi D., Reiter M.K., “On k-set Consensus Problems in Asynchronous Systems”, PODC ’99 Proceedings of the eighteenth annual ACM symposium on Principles of distributed computing, str. 257-265, ACM New York, ISBN: 1-58113-099-6, <https://www.cs.unc.edu/~reiter/papers/1999/PODC.pdf>, (dostęp: 03.06.2016r.) [↑](#endnote-ref-8)
9. Sape Mullender, Distributed Systems, Addison-Wesley; 2 edition (June 30, 1993),ISBN-13: 978-0201624274 [↑](#endnote-ref-9)
10. Aguilera M.K., Toueg S., “Correctness Proof of Ben-Or’s Randomized Consensus Algorithm”, Proceedings of the 10th International Workshop on Distributed Algorithms, Springer-Verlag, <http://disi.unitn.it/~montreso/ds/syllabus/papers/AguileraToeug-CorrecnessBenOr.pdf>, (dostęp: 04.06.2016r.) [↑](#endnote-ref-10)
11. Coulouris G., Dollimore J., Kindberg T., Gordon B., “Distributed Systems. Concepts and Design. Fifth Edition”, str. 662, Pearson Education, 2012, Boston [↑](#endnote-ref-11)
12. Mads Dam, “Parallel and Distributed Computing. Distributed Algorithms. Lecture 7: Consensus”, slajdy 72-82 oraz 93, <http://www.csc.kth.se/utbildning/kth/kurser/DD2451/pardis11/DD2451_lecture7.pdf>, (dostęp: 26.05.2016) [↑](#endnote-ref-12)
13. Nelson M., “The Byzantine Generals Problem”, artykuł: <http://marknelson.us/2007/07/23/byzantine/>, (dostęp: 22.05.2016) [↑](#endnote-ref-13)
14. “Systemy Równoległe i rozproszone”, wykład nr 13 – „Rozgłaszanie i uzgadnianie”, strona z materiałami dydaktycznymi dr hab. inż. K. Banasia, <http://www.metal.agh.edu.pl/~banas/SRR/SRR_W13_Rozglaszanie_Uzgadnianie.pdf>, (dostęp: 22.05.2016) [↑](#endnote-ref-14)
15. Ajay Kschemkalyani, Mukesh Singhal, „Distributed Computing: Principles, Algorithms and Systems. Chapter 14: Consensus and Agreement”, Cambridge University Press, <https://www.cs.uic.edu/~ajayk/Chapter14.pdf>(dostęp: 22.05.2016) [↑](#endnote-ref-15)
16. Mads Dam, “Parallel and Distributed Computing. Distributed Algorithms. Lecture 7: Consensus”,slajdy 48-55, <http://www.csc.kth.se/utbildning/kth/kurser/DD2451/pardis11/DD2451_lecture7.pdf>, (dostęp: 22.05.2016) [↑](#endnote-ref-16)
17. „Computer Science & Engineering. Courses. CSEP552: Distributed Systems.Lecture 5: Intro to consensus”, University of Washington, <http://courses.cs.washington.edu/courses/csep552/13sp/lectures/5/intro.pdf> (dostęp 21.05.2016) [↑](#endnote-ref-17)
18. Paul Krzyzanowski, „Consensus. Reaching agreement”, <https://www.cs.rutgers.edu/~pxk/417/notes/content/consensus.html>(dostęp: 22.05.2016) [↑](#endnote-ref-18)
19. <https://www.cs.uic.edu/~ajayk/Chapter14.pdf> (dostęp 26.05.2016) [↑](#endnote-ref-19)
20. <https://www.cs.unc.edu/~reiter/papers/1999/PODC.pdf> (dostęp 26.05.2016) [↑](#endnote-ref-20)