Chapter 18
Broadcast & Shared Coins

In Chapter 17 we have developed a fast solution for synchronous byzantine agreement (Algorithm 17.14), yet our asynchronous byzantine agreement solution (Algorithm 17.21) is still awfully slow. Some simple methods to speed up the algorithms did not work, mostly due to unrealistic assumptions. Can we at least solve asynchronous (assuming worst-case scheduling) consensus if we have crash failures? Possibly based on some advanced communication methods?

18.1 Shared Coin on a Blackboard

Definition 18.1 (Shared Coin). A shared coin is a binary random variable shared among all nodes. It is 0 for all nodes with constant probability and 1 for all nodes with constant probability. The shared coin is allowed to fail (be 0 for some nodes and 1 for other nodes) with constant probability.

Remarks:
- In Chapter 16, we have already seen a shared coin in Algorithm 16.21. For that shared coin, we implicitly assumed that message scheduling was random.
- Worst-case scheduling is an issue that we have only briefly considered so far, in particular, to show that the random bitstring does not help so far.
- In Algorithm 18.4 the outcome of a coinflip is ±1 or ±1 instead of 0 or 1 because it simplifies the analysis, i.e., "−1 ± 0".
- The sign function is used for the decision values. The sign function returns +1 if the sum of all coinflips in C is positive, and −1 if it is negative.
- The algorithm is unusual compared to other asynchronous algorithms we have dealt with so far. So far we often waited for n − f messages from other nodes. In Algorithm 18.4, a single node can single-handedly generate all n² coinflips, without waiting.
- If a node does not need to wait for other nodes, we call the algorithm wait-free.
- Many similar definitions beyond wait-free exist: lock-free, deadlock-free, starvation-free, and generally non-blocking algorithms.

Theorem 18.5 (Central Limit Theorem). Let \(\{X_1, X_2, \ldots, X_N\}\) be a sequence of independent random variables with \(Pr[X_i = -1] = Pr[X_i = 1] = 1/2\) for all \(i = 1, \ldots, N\). Then for every positive real number \(z\),

\[
\lim_{N \to \infty} Pr \left[ \sum_{i=1}^{N} X_i \geq z\sqrt{N} \right] = 1 - \Phi(z) > \frac{1}{\sqrt{2\pi}} \cdot \frac{2}{z} \cdot e^{-z^2/2},
\]

where \(\Phi(z)\) is the cumulative distribution function of the standard normal distribution evaluated at \(z\).
Theorem 18.6. Algorithm 18.4 implements a polynomial shared coin.

Proof. Each node in the algorithm terminates when at least $n^2$ coinflips are written to the blackboard. Before terminating, nodes may write one additional coinflip. Therefore, every node decides after reading at least $n^2$ and at most $n^2 + n$ coinflips. The power of the adversary lies in the fact that it can prevent $n - 1$ nodes from writing their coinflips to the blackboard by delaying their writes. Assume that the fastest node finishes with the result $+1$ after reading $n^2$ coinflips. In the worst case, each of the remaining $n - 1$ nodes will write $-1$ to the memory before finishing. This way, the sum of all coinflips that are used for decision might deviate by $n - 1$.

We need to show that both outcomes for the shared coin ($+1$ or $-1$ in Line 6) will occur with constant probability, as in Definition 18.1. Let $X$ be the sum of all coinflips that are visible to every node. Since some of the nodes might read $n$ more values from the blackboard than others, the nodes cannot be prevented from deciding if $|X| > n$. By applying Theorem 18.5 with $N = n^2$ and $z = 1$, we get:

$$
Pr(X < -n) = Pr(X > n) = 1 - \Phi(1) > 0.15.
$$

Lemma 18.7. Algorithm 18.4 uses $n^2$ coinflips, which is optimal in this model.

Proof. The proof for showing quadratic lower bound makes use of configurations that are indistinguishable to all nodes, similar to Theorem 16.13. It requires involved stochastic methods and we therefore will only sketch the idea of where the $n^2$ comes from.

The basic idea follows from Theorem 18.5. The standard deviation of the sum of $n^2$ coinflips is $n$. The central limit theorem tells us that with constant probability the sum of the coinflips will be only a constant factor away from the standard deviation. As we showed in Theorem 18.6, this is large enough to disarm a worst-case scheduler. However, with much less than $n^2$ coinflips, a worst-case scheduler is still too powerful. If it sees a positive sum forming on the blackboard, it delays messages trying to write $+1$ in order to turn the sum temporarily negative, so the nodes finishing first see a negative sum, and the delayed nodes see a positive sum.

Remarks:
- Algorithm 18.4 cannot tolerate even one byzantine failure: assume the byzantine node generates all the $n^2$ coinflips in every round due to worst-case scheduling. Then this byzantine node can make sure that its coinflips always sum up to a value larger than $n$, thus making the outcome $-1$ impossible.
- In Algorithm 18.4, we assume that the blackboard is a trusted central authority. Like the random oracle of Definition 17.24, assuming a blackboard does not seem practical. However, fortunately, we can use advanced broadcast methods in order to implement something like a blackboard with just messages.

18.2 Broadcast Abstractions

Definition 18.8 (Accept). A message received by a node $v$ is called accepted if node $v$ can consider this message for its computation.

Definition 18.9 (Best-Effort Broadcast). Best-effort broadcast ensures that a message that is sent from a correct node $u$ to another correct node $v$ will eventually be received and accepted by $v$.

Remarks:
- Note that best-effort broadcast is equivalent to the simple broadcast primitive that we have used so far.
- Reliable broadcast is a stronger paradigm which implies that Byzantine nodes cannot send different values to different nodes. Such behavior will be detected.

Definition 18.10 (Reliable Broadcast). Reliable broadcast ensures that the nodes eventually agree on all accepted messages. That is, if a correct node $v$ considers message $m$ as accepted, then every other node will eventually consider message $m$ as accepted.

Algorithm 18.11 Asynchronous Reliable Broadcast (code for node $u$)

```
1: Broadcast own message msg(u)
2: upon receiving msg(v) from $v$ or echo(w, msg(v)) from $n - 2f$ nodes $w$: 
3: Broadcast echo(u, msg(v))
4: upon receiving echo(w, msg(v)) from $n - f$ nodes $w$: 
5: Accept msg(v)
```

Theorem 18.12. Algorithm 18.11 satisfies the following properties:

1. If a correct node broadcasts a message reliably, it will eventually be accepted by every other correct node.
2. If a correct node has not broadcast a message, it will not be accepted by any other correct node.
3. If a correct node accepts a message, it will be eventually accepted by every correct node.

This algorithm can tolerate $f < n/3$ Byzantine nodes or $f < n/2$ crash failures.

Proof. We start with the first property. Assume a correct node broadcasts a message $msg(v)$, then every correct node will receive $msg(v)$ eventually. In Line 3, every correct node (including the originator of the message) will echo the message and, eventually, every correct node will receive at least $n - f$ echoes, thus accepting $msg(e)$.

The second property holds for the case with crash failures, as all correct nodes follow the algorithm. In the Byzantine case, Byzantine nodes are not able to forge an incorrect sender address, see Definition 17.1. Instead, they can echo messages from correct nodes with a wrong input value. If all Byzantine nodes...
18.2. BROADCAST ABSTRACTIONS

Echo a message that has not been broadcast by a correct node, each correct node will receive at most $f < n - 2f$ echo messages and thus no correct node will accept such a message.

For the third property, assume that some message originated from a byzantine node $b$, or a node $b$ that has crashed in the process of sending its message. If a correct node accepted message $\text{msg}(b)$, this node must have received at least $n - f$ echoes for this message in Line 4. If at most $f$ nodes are faulty, at least $n - 2f$ correct nodes must have broadcast an echo message for $\text{msg}(b)$. Therefore, every correct node will receive these $n - 2f$ echoes eventually and will broadcast an echo. Finally, all $n - f$ correct nodes will have broadcast an echo for $\text{msg}(b)$ and every correct node will accept $\text{msg}(b)$.

Remarks:
- Algorithm 18.11 does not solve consensus according to Definition 16.1. It only makes sure that all messages of correct nodes will be accepted eventually. For correct nodes, this corresponds to sending and receiving messages in the asynchronous time model (Model 16.2).
- The algorithm has a linear message overhead since every node again broadcasts every message.
- Note that byzantine nodes can issue arbitrarily many messages. This may be a problem for protocols where each node is only allowed to send one message (per round). Can we fix this, for instance with sequence numbers?

Definition 18.13 (FIFO Reliable Broadcast). The FIFO (reliable) broadcast defines an order in which the messages are accepted in the system. If a node $u$ broadcasts message $m_1$ before $m_2$, then any node $v$ will accept message $m_1$ before $m_2$.

Algorithm 18.14 FIFO Reliable Broadcast (code for node $u$)

1. Broadcast own round $r$ message $\text{msg}(u, r)$
2. Upon receiving first message $\text{msg}(v, r)$ from node $v$ for round $r$ or $n - 2f$
3. Broadcast echo($u, \text{msg}(v, r))$
4. Upon receiving echo($u, \text{msg}(v, r))$ from $n - f$ nodes $w$:
5. If accepted $\text{msg}(v, r)$ then
6. Accept $\text{msg}(v, r)$
7. End if

Theorem 18.15. Algorithm 18.14 satisfies the properties of Theorem 18.12. Additionally, Algorithm 18.14 makes sure that no two messages $\text{msg}(v, r)$ and $\text{msg}(v', r)$ are accepted from the same node. It can tolerate $f < n/3$ byzantine nodes or $f < n/2$ crash failures.

Proof. Just as reliable broadcast, Algorithm 18.14 satisfies the three properties of Theorem 18.12 by simply following the flow of messages of a correct node. It remains to show that at most one message will be accepted from some node $v$ in round $r$. In the crash failure case, this property holds because all nodes follow the algorithm and therefore send at most one message in a round. For the byzantine case, consider some correct node $u$ that has accepted $\text{msg}(v, r)$ in Line 6. This node must have received $n - f$ echoes for this message, $n - 2f$ of which were the first echoes of the correct nodes. Assume for contradiction that another correct node accepts $\text{msg}'(v, r)$. This node must have collected $n - f$ messages $\text{echo}(w, \text{msg}(v, r))$. Since at least $n - 2f$ of these messages must be the first echo messages sent by correct nodes, we have $n - 2f + n - 2f = 2n - 4f < n - f$ (for $f < n/3$) echo messages sent by the correct nodes as their first echo. This is a contradiction.

Definition 18.16 (Atomic Broadcast). Atomic broadcast makes sure that all messages are received in the same order by every node. That is, for any pair of nodes $u, v$, and for any two messages $m_1$ and $m_2$, node $u$ receives $m_1$ before $m_2$ if and only if node $v$ receives $m_1$ before $m_2$.

Remarks:
- Definition 18.16 is equivalent to Definition 15.8, i.e., atomic broadcast = state replication.
- Now we have all the tools to finally solve asynchronous consensus.

18.3 Blackboard with Message Passing

Algorithm 18.17 Simulating a write to the blackboard (code for node $u$)

1. FIFO-broadcast $\text{msg}(u)$ to all nodes
2. Participate in FIFO-broadcast of all messages and write all received messages to a local blackboard
3. Wait until accepted own $\text{msg}(u)$

Algorithm 18.18 Simulating a read from the blackboard (code for node $u$)

1. Request local blackboards from all nodes
2. Wait for $u - f$ responses and add all newly seen messages to own local blackboard

Theorem 18.19. Algorithm 18.14 together with the write operation from Algorithm 18.17 and the read operation from Algorithm 18.18 solves asynchronous binary agreement for $f < n/2$ crash failures.

Proof. The upper bound for the number of crash failures results from the upper bound in Theorem 18.15. Algorithm 18.17 simulates a write operation: by accepting the own message/coinflip, a node verifies that $n - f$ nodes have received its most recent generated coinflip $\text{coin}(c_u)$ and written it to their local blackboard. At least $n - 2f > 1$ of these nodes will never crash and the value therefore can be considered as stored on the blackboard. While $u$’s own value is not accepted and
18.4 USING CRYPTOGRAPHY 177
therefore not stored, node u will not generate new coinflips. Therefore, at any
point of the algorithm, there are at most n additional generated coinflips next
to the accepted coins. This corresponds to the write operation in Algorithm
18.4.
Algorithm 18.18 simulates a read operation from the blackboard. A node
reads a value by receiving the local views of the blackboards from at least
n − f nodes. Note that each written value is stored on n − f local blackboards.
Therefore, a node will see at least (n − f) + (n − f) − n = n − 2f > 1 copies of
each value that was written to the blackboard so far.
This shows that the read and write operations are equivalent to the same op-
erations in Algorithm 18.4. Assume now that some correct node has terminated
after reading n2 coinflips. Since each node reads the stored coinflips before gen-
erating a new one in the next round, there will be at most n additional coins
accepted by any other node before termination. This setting is equivalent to
Theorem 18.6 and the rest of the analysis is therefore analogous to the analysis
in that theorem.
□
Remarks:
• So finally we can deal with worst-case crash failures and worst-case
   scheduling.
• But what about byzantine agreement? We need even more powerful
   mechanisms!

18.4 Using Cryptography

Definition 18.20 (Threshold Secret Sharing). Let t, n ∈ N with 1 ≤ t ≤ n.
An algorithm that distributes a secret among n participants such that t partici-
pants need to collaborate to recover the secret is called a (t, n)-threshold secret
sharing scheme.

Definition 18.21 (Signature). Every node can sign its messages in a way that
no other node can forge, thus nodes can reliably determine which node a
signed message originated from. We denote a message x signed by node u with
\( \text{sign}(x)_u \).

Algorithm 18.22 (t, n)-Threshold Secret Sharing

1: Input: A secret s, represented as a real number.
   Secret distribution by dealer d
2: Generate t − 1 random numbers \( a_1, \ldots, a_{t-1} \in \mathbb{R} \)
3: Obtain a polynomial \( p \) of degree \( t-1 \) with \( p(x) = s + a_1x + \cdots + a_{t-1}x^{t-1} \)
4: Generate n distinct \( x_1, \ldots, x_n \in \mathbb{R} \setminus \{0\} \)
5: Distribute share \( \text{msg}(x_i, p(x_i))_d \) to node \( v_1, \ldots, \text{msg}(x_n, p(x_n))_d \) to node \( v_n \)
   Secret recovery
6: Collect t shares \( \text{msg}(x_i, p(x_i))_u \) from at least t nodes
7: Use Lagrange's interpolation formula to obtain \( p(0) = s \)

Algorithm 18.23 Preprocessing Step for Algorithm 18.24 (code for dealer d)

1. According to Algorithm 18.22, choose polynomial \( p \) of degree \( f \)
2. for \( i = 1, \ldots, n \) do
   3. Choose coinflip \( c_i \), where \( c_i = 0 \) with probability \( 1/2 \), else \( c_i = 1 \)
   4. Using Algorithm 18.22, generate n shares \( (x'_1, p(x'_1)), \ldots, (x'_n, p(x'_n)) \) for
      \( c_i \)
   5. end for
   6. Send shares \( \text{msg}(x'_1, p(x'_1))_d, \ldots, \text{msg}(x'_n, p(x'_n))_d \) to node \( u \)

Algorithm 18.24 Shared Coin using Secret Sharing (ith iteration)

1. Replace Line 12 in Algorithm 17.21 by
2. Request shares from at least \( f + 1 \) nodes
3. Using Algorithm 18.22, let \( c_i \) be the value reconstructed from the shares
4. return \( c_i \)

Theorem 18.25. Algorithm 17.24 together with Algorithm 18.23 and Algo-
rimth 18.24 solves asynchronous byzantine agreement for \( f < n/3 \) in expected 3
number of rounds.

Proof. In Line 2 of Algorithm 18.24, the nodes collect shares from \( f + 1 \) nodes.
Since a byzantine node cannot forge the signature of the dealer, it is restricted
to either send its own share or decide not to send it at all. Therefore, each
correct node will eventually be able to reconstruct secret \( c_i \) of round \( i \) correctly
in Line 3 of the algorithm. The running time analysis follows then from the
analysis of Theorem 17.26.
□
Remarks:
• In Algorithm 18.23 we assume that a dealer generates the random
   bitstring. This assumption is not necessary if the communication be-
tween any pair of nodes is private: In a setup phase of the algorithm,
   each node can generate a local coinflip and broadcast the secret shares
   of its coinflip to all other nodes. The corresponding secret will only
   be revealed in a designated round of the algorithm, thus keeping the
   outcome of the coinflip secret to a byzantine adversary.
We showed that cryptographic assumptions can speed up asynchronous byzantine agreement.
Algorithm 17.21 can also be implemented in the synchronous setting.
A randomized version of a synchronous byzantine agreement algorithm can improve on the lower bound of \( t + 1 \) rounds for the deterministic algorithms.

**Definition 18.26** (Cryptographic Hash Function). A hash function function \( h : U \rightarrow S \) is called cryptographic, if for a given \( z \in S \) it is computationally hard to find an element \( x \in U \) with \( h(x) = z \).

**Remarks:**
- Popular hash functions used in cryptography include the Secure Hash Algorithm (SHA) and the Message-Digest Algorithm (MD).

**Algorithm 18.27** Simple Synchronous Byzantine Shared Coin (for node \( u \))

1. Each node has a public key that is known to all nodes.
2. Let \( r \) be the current round of Algorithm 17.21
3. Broadcast \( \text{msg}(r)_v \), i.e., round number \( r \) signed by node \( v \)
4. Compute \( h_u = h(\text{msg}(r)_v) \) for all received messages \( \text{msg}(r)_v \)
5. Let \( h_{\min} = \min_u h_u \)
6. return least significant bit of \( h_{\min} \)

**Remarks:**
- In Algorithm 18.27, Line 3 each node can verify the correctness of the signed message using the public key.
- Just as in Algorithm 17.9, the decision value is the minimum of all received values. While the minimum value is received by all nodes after 2 rounds there, we can only guarantee to receive the minimum with constant probability in this algorithm.
- Hashing helps to restrict byzantine power since a byzantine node cannot compute the smallest hash.

**Theorem 18.28.** Algorithm 18.27 plugged into Algorithm 17.21 solves synchronous byzantine agreement in expected 5 rounds for up to \( f < n/10 \) byzantine failures.

**Proof.** With probability 1/3 the minimum hash value is generated by a byzantine node. In such a case, we can assume that not all correct nodes will receive the byzantine value and thus, different nodes might compute different values for the shared coin.

With probability 2/3, the shared coin will be from a correct node, and with probability 1/2 the value of the shared coin will correspond to the value which was deterministically chosen by some of the correct nodes. Therefore, with probability 1/3 the nodes will reach consensus in the next iteration of Algorithm 17.21. The expected number of rounds is:

\[
1 + \sum_{i=0}^{\infty} 2 \left( \frac{2}{3} \right)^i = 5
\]

**Chapter Notes**

Asynchronous byzantine agreement is usually considered in one out of two communication models – shared memory or message passing. The first polynomial algorithm for the shared memory model that uses a shared coin was proposed by Aspnes and Herlihy [AH90] and required exchanging \( O(n^2) \) messages in total. Algorithm 18.4 is also an implementation of the shared coin in the shared memory model and it requires exchanging \( O(n^3) \) messages. This variant is due to Saks, Shavit and Woll [SSW91]. Bracha and Rachman [BR92] later reduced the number of messages exchanged to \( O(n \log n) \). The tight lower bound of \( \Omega(n^2) \) on the number of coinflips was proposed by Attiya and Censor [AC98] and improved the first non-trivial lower bound of \( \Omega(n^2 / \log n) \) by Aspnes [Asp98].

In the message passing model, the shared coin is usually implemented using reliable broadcast. Reliable broadcast was first proposed by Reischuk and Toueg [ST87] as a method to simulate authenticated broadcast. There is also another implementation which was proposed by Bracha [Bra87]. Today, a lot of variants of reliable broadcast exist, including Fifio broadcast [AAD05], which was considered in this chapter. A good overview of the broadcast routines is given by Cachin et al. [CGR14]. A possible way to reduce message complexity is by simulating the read and write commands [ABD95] as in Theorem 18.19. The message complexity of this method is \( O(n^2) \). Alistarh et al. [AAKS14] improved the number of exchanged messages to \( O(n \log^2 n) \) using a binary tree that restricts the number of communicating nodes according to the depth of the tree.

It remains an open question of whether asynchronous byzantine agreement can be solved efficiently in the message passing model without cryptographic assumptions. If cryptographic assumptions are however used, byzantine agreement can be solved in expected constant number of rounds. Algorithm 18.23 presents the first implementation due to Rabin [Rab83] using threshold secret sharing. This algorithm relies on the fact that the dealer provides the random bitstring. Chor et al. [CGMA85] proposed the first algorithm where the nodes use verifiable secret sharing in order to generate random bits. Later work focuses on improving resiliency [CR00] and practicality [CKS00]. Algorithm 18.27 by Micali [Mic98] shows that cryptographic assumptions can also help to improve the running time in the synchronous model.

This chapter was written in collaboration with Darya Melnyk.

**Bibliography**

[AAD05] Ittai Abraham, Yonatan Amit, and Danny Dolev. Optimal resilience asynchronous approximate agreement. In Proceedings of the


