A PROTOCOL FOR ELECTRONIC MONEY

STORE, CUSTOMER, AND BANK WHERE:

1. The customer may decide to pay. That is, the customer sends the money to the store.
2. The customer may decide to cancel. The money is sent to the bank with a message that the value of the money is to be added to the customer's bank account.
3. The store may ship goods to the customer.
4. The store may redeem the money. That is, the money is sent to the bank with a request that its value be given to the store.
5. The bank may transfer the money by creating a new, suitably encrypted money file and sending it to the store.

![Diagram](image)

Figure 2.1: Finite automata representing a customer, a store, and a bank

(a) Store
(b) Customer
(c) Bank

Figure 2.2: The complete set of transitions for the three automata

However, in order to use electronic money, protocols need to be devised to allow the manipulation of the money in a variety of ways that the users want. Because monetary systems always invite fraud, we must verify whatever policy we adopt regarding how money is used. That is, we need to prove the only things that can happen are things we intend to happen — things that do not allow an unscrupulous user to steal from others or to “manufacture” money.

In the balance of this section, we shall introduce a very simple example of an electronic-money protocol, model it with finite automata, and show how constructions on automata can be used to verify protocols (or, in this case, to discover that the protocol has a bug).

2.1.1 The Ground Rules

There are three participants: the customer, the store, and the bank. We assume for simplicity that there is only one “money” file in existence. The customer may decide to transfer this money file to the store, which will then redeem the file from the bank (i.e., get the bank to issue a new money file belonging to the store rather than the customer) and ship goods to the customer. In addition, the customer has the option to cancel the file. That is, the customer may ask the bank to place the money back in the customer's account, making the money no longer spendable.