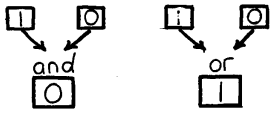
Kopf oder Zahl über große Distanzen

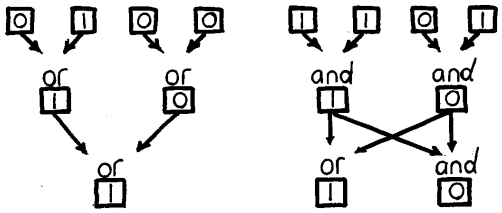
Modifizierte Übersetzung von »The Peruvian Coin Flip« aus `http://csunplugged.org`.

Die Handballteams aus Berlin und Essen müssen auslosen, bei wem das Spiel zwischen den beiden Mannschaften ausgetragen werden soll. Melissa für Berlin und Anika für Essen wurde diese Aufgabe übertragen. Sie haben aber nicht die Zeit und das Geld sich irgendwo für die Auslosung zu treffen. Können sie es am Telefon machen? Melissa wirft die Münze und Anika wählt zwischen Kopf und Zahl. Dieses funktioniert aber nicht, denn wenn Anika Zahl wählt, kann Melissa einfach sagen „Es ist Kopf“ und Anika kann es nicht überprüfen.

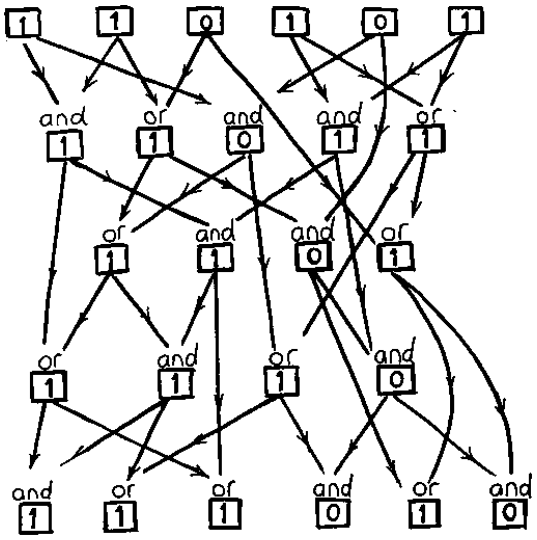
Beide einigen sich auf eine Möglichkeit: Sie erarbeiten zusammen eine Schaltung aus Und- und Oder-Gliedern, was sich auch am Telefon oder per E-Mail realisieren lässt. Bei der Erstellung haben beide ein Interesse daran, dass die Schaltung komplex genug ist, dass die andere sie nicht knacken kann. Die Schaltung, die zum Schluss genutzt wird, ist öffentlich.



Die Regeln für ein Und- und Oder-Glied sind einfach. Jedes Glied hat zwei Eingaben und eine Ausgabe. Jede Eingabe kann 1 oder 0 sein, was sich auch als ja oder nein interpretieren lässt. Die Ausgabe von einem Und-Glied ist 1(ja), wenn beide Eingaben 1(ja) sind. Andernfalls ist die Ausgabe 0(nein). Als Beispiel hat das Und-Glied eine 0 und eine 1 als Eingabe, was oben drüber geschrieben wird. Dann ist die Ausgabe 0, was in das Quadrat unten drunter geschrieben wird. Die Ausgabe eines Oder-Glieds ist 1, wenn beide oder eine der beiden Eingaben 1 ist. Sie ist nur dann 0, wenn beide Eingaben 0 sind. So ist die Ausgabe für das Oder-Glied 1, wenn eine 1 und eine 0 eingegeben werden.



Der Ausgang von einem Glied kann mit dem Eingang eines oder mehrerer anderer Glieder verbunden werden, um kompliziertere Effekte zu erhalten. Im Beispiel sind bei der linken Schaltung zwei Oder-Glieder mit einem dritten Oder-Glied verbunden. Dieses hat den Effekt, dass 1 herauskommt, sobald eine der Eingaben auch 1 ist. In der rechten Schaltung sind die Ausgänge von jedem der oberen zwei Und-Glieder jeweils mit einem Und- und einem Oder-Glied verbunden, so dass die Schaltung zwei Ausgaben hat.

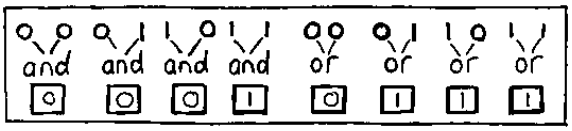


Für das Kopf-Zahl-Problem wird eine komplexere Schaltung benötigt. Diese hat sechs Ein- und sechs Ausgaben. Hier rechts ist ein Beispiel für eine mögliche Kombination von Eingaben. Diese Schaltung kann nun wie folgt bei dem Anruf genutzt werden: Melissa wählt eine zufällige Eingabe, bestehend aus sechs Ziffern für die Schaltung aus, die sie geheim hält. Für diese Eingabe bestimmt sie die Ausgabe und gibt die Ausgabe an Anika. Dann rät Anika, ob die Eingabe von Melissa eine ungerade oder gerade Anzahl von Einsen enthält – In anderen Worten die Parität. Wenn die Schaltung komplex genug ist, kann Anika nicht von der Ausgabe auf die Eingabe schließen und sie muss die Parität raten (Oder

eine Münze werfen). Anika gewinnt, wenn ihre Wahl korrekt ist und sonst gewinnt Melissa. Dazu muss Anika nur ihre Wahl der Melissa mitteilen und anschließend Melissa ihre geheime Eingabe. So kann Anika die angegebene Ausgabe überprüfen.

Aufgabe

1. Setze dich mit einem Partner zusammen und wendet gemeinsam das Verfahren mehrfach an. Nutzt dafür die unteren Graphiken. Die Regeln der Glieder sind hier noch mal angegeben:



2. Finde heraus, ob Anika mogeln kann, indem sie die Eingabe aus der Ausgabe herausfindet. In diesem Fall wäre die Schaltung keine Einwegfunktion. Schreibe auf, was eine Einwegfunktion ist.
3. Suche Möglichkeiten, mit denen Melissa schummeln kann. So muss für Eingaben mit gerader und ungerader Anzahl Einsen die gleiche Ausgabe herauskommen.
4. Erstelle mit dem Partner eine eigene Schaltung und probiert diese aus. Gib an, ob es hier für Anika oder Melissa einfacher ist zu schummeln.