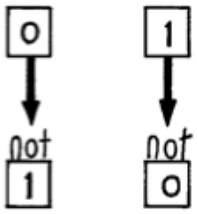

図 17.4 The not-gate(YET)

だから、もしこの数をアリシアが偶然思いついたなら、ベニートは偶数とあてることができ、しかも正しいと確信できるのです。

コンピュータシステムを使うと、もっとたくさんのビットを使って、非常にたくさんの可能性を試すことができます。(ビットを増やすと数の可能性は 2 倍になります)

さあ、子供たちのグループにこのゲームのための彼ら自身の回路を発明させましょう。

アリシアのために、、そしてもう一方はベニートのために簡単にだます回路をみつけることができるでしょうか。

回路がなぜ 6 つの入力を持つかどうかは問題ではなく、違った数の入力と出力でもできるでしょう。

Variations and extensions
変化と拡張

1. この実践でのはっきりした課題は、連携してアリシアとベニートの両方に受け入れられる回路を作る必要があることです。

この学習は子供たちには楽しいかもしれませんが、特に電話越しでは実行ができないような手順を示してしまいがちです。

だけど、アリシアとベニートがそれぞれ回路を作成し、公開するという簡単な選択肢もあります。

その時、アリシアは秘密の数を両方の回路に通し、２つの出力を併せて比較し、同じなら 1 、違うなら 0 というように合わせて最終的な出力を作ります。

この状況では、回路の 1 つが一方向関数の場合、合成したものも一方向関数なので、どちらも騙せないし、騙されないのです。

次の２つの変化形は暗号化プロトコルやコイン投げにはある意味関係ないですが、どちらかと言うと AND 回路や OR 回の出力から作られる回路の考え方なのです。

彼らはコンピュータ回路だけでなく、論理そのものに至るまで、基本にあるいくつかの重要な考えを調査しました。

この種の論理は数学者ジョージ・ブールにちなんでブール代数と呼ばれています。

子供たちは、すべて 0 の入力 000000 は必ずすべて 0 の出力になり、同様にすべて 1 の入力 111111 はすべて 1 の出力になることに気がついたでしょうか。

(他の入力でもこの出力と同じ結果になるものもあります：実際の例として 000010 はすべて 0 になり、110111 はすべて 1 になります。)

これは、回路が AND 回路と OR 回路から作られているという事実の帰結です。

入力したものに対して反対のものを出力する NOT 回路（図 17.4）を加えることで、子供たちはこの性質を持たない回路を作ることができるのです。

3. 別の２つの重要な回路は AND 回路や NOT 回路のようでもあるが、NOT 回路で生成された NAND 回路と NOR 回路です。

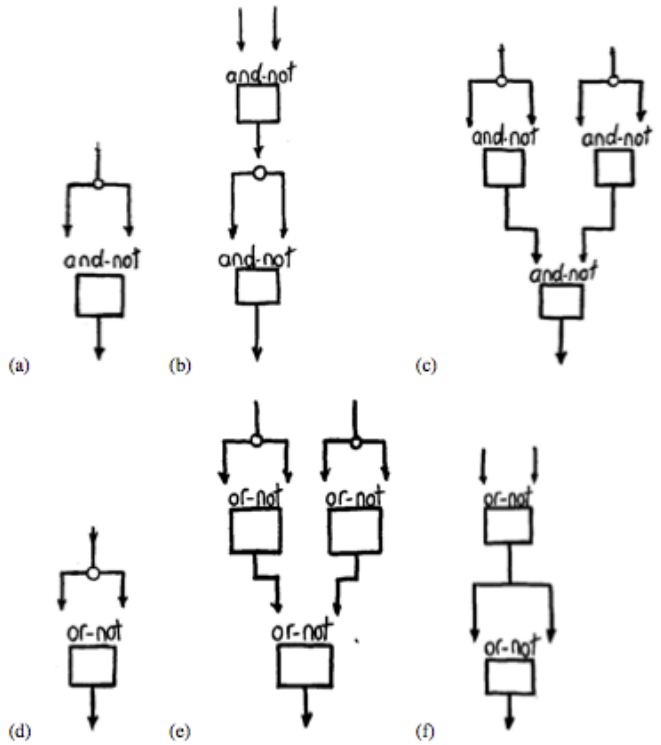

図 17.5　Making the three basic gates from and-not and or-not gates. (a) and (d) are not- gates, (b) and (e) are and-gates, while (c) and (f) are or-gates.(YET)

ゆえに、a NAND b は（a かつ b) の否定です。

出力結果が常に AND 回路、OR 回路、NOT 回路で置き換えることで得られるので、これらは関数的な違いがないと考えられます。

また一方で、任意の回路は複数の NAND 回路または複数の NOT 回路で作ることができるという興味深い特徴を持ちます。

もしそれらがたった 1 つの種類の回路が繋がったものだと彼等が発見できたなら、NAND 回路と NOR 回路を紹介することで、子供たちにどんな回路も別の回路と繋がること、さらには互いに繋がっているのがたった 1 種類の回路であることを発見させることに挑戦させましょう。

図 17.5 はの上の行は、３つの基本的な回路である AND 回路、OR 回路、NOT 回路が NAND 回路から作られることを示していて、下の行は NOR 回路から作られることを示しています。

What’s it all about?
いったい何？

ここ数年、コンピュータネットワークを通じて行われる商業取引の量が増加し、電子決済や部外秘の取引、署名、法的拘束力のある、文書などの安全な交換を保証することがどうしても必要なのです。

暗号学のデーマは安全で非公開の方式での通信についてです。

20 年前、コンピュータ科学の研究者は次のような直感では考えられない結果を発見しました。それは、確かな情報は公開され続けていることを保証する技術により、セキュリティが保証されているということです。

その結果は学習 18 Kid Krypto にある「公開鍵暗号」と呼ばれ今や情報を交換する唯一の完全な安全路と考え

られています。

暗号学は物事を秘密にすることについてだけではなく、他人が見つけることができる限界を管理することや、距離的に離れている人と人との間の信頼を確立することについて（研究）します。

暗号取引のための正式な規則もしくは「プロトコル」は、次のような一見不可能なことを許可するために発明された。それは偽造不可能な電子署名、何をしているか実際に明かすことない秘密を保つこと（パスワードのように）を他の人に伝える能力などです。

電話でのコイン投げは簡単ですが、一見不可能そうに見える点で似通った問題です。

実際の状況では、アリシアとベニートは自分たちでは回路を作ることはしないでしょうが、内部で変換してくれるコンピュータプログラムを得るでしょう。

おそらく、誰もソフトウェアの内部には興味を持たないでしょう。

しかし、どんなにコンピュータ技術が素晴らしく、どんなに一生懸命試みても、決定の結果に影響を与えることができないという安心をどちらもしたいでしょう。

原則として、どんな議論も公平な判定者に訴えることにより解決されなければならない。

判定は 回路図やアリシアの作った２進数、ベニートに送った出力値、そしてお返しにベニートが送った予想から導き出されます。

ひとたび交換が終われば、これら全ては公開された情報で、双方の参加者は結果が基づいているものとして賛成する必要があります。

判定はアリシアの数を回路に通し、出力が言った通りであることを確認し、その結果決定が正しいかどうかを判定します。

言うまでもなく、規則をチェックする明確な手順があるという事実は、論争がおこることはありそうもないということにつながります。

アリシアが実物の硬貨を投げ、ベニートが表か裏をあてる状況と比較してみると、その場合には判定はありません。

騙すために、表 17.1 を見つけ出すことは簡単なので、人が描いたような小さい回路は実際にはめったに使われません。

入力するのに 30 ケタの 2 進数を使うことは保護の度合いが高くなります。

しかし、これすらも特定の回路に依存するので、騙すことが難しいことを保証しません。

学習 14 Tourist Town で紹介した一方向関数のような他の方式を使うことができました。

実際に使われた方式は難しい問題として知られている大きな数の素因数分解によく左右されます。(次の学習の最後で学ぶように、それは NP-complete ではありません)

1 つの数が別の数の因数であることを調べるのは簡単ですが、大きな数の因数を見つけることは大変時間がかかります。

アリシアとベニート（判定も）にとっても、人手で行うはあまりにも複雑なので、前に書いたように実際は既成のソフトウェア上で行います。

電子署名は同じようなアイデアに基づいています。

アリシアが選んだ特別な秘密の入力に対する回路の出力を公開することで、正しい一方向関数を使って、出力を生成したのは自分であることを効果的に証明します。そして他の人は誰も入力値を見つけることができません。

アリシアになりすますことはできません！

実際の電子署名を生成するには、アリシアが特別なメッセージに署名できること、さらに彼女がそうでないと偽ったとしても誰もがアリシアの署名だと確認できることをもっと複雑な約束で証明する必要があります。

しかし基本は同じです。

もう 1 つの活用としてカードを扱ったり、プレイヤーの手を記録する親がいない電話回線を使ったポーカーがあります。

ゲームの終わりにトラブルが生じた場合、判定により、プレイヤー自身ですべては実行できるに違いありません。

同様の状況が契約交渉？ の始めに起きます。

もちろん、プレイヤーはゲームをしている間カードを秘密にしなければなりません。

しかし、トランプのエースを持つ前に、エースを持っているというように騙すことは許されず、ずっと正直でいなければなりません。

これは、ゲームが終わるまで待たされことにより検査することができ、それぞれのプレーヤーに相手方の手と手順を検査することが許されます。

もう１つの問題は、それぞれのプレーヤーの手が秘密である間、ゲーム後までどうやってカードを扱うかです。

意外にも、コイン投げと似ていなくはない暗号化プロトコルを使うことで、それを成し遂げるのは可能なのです。

暗号化プロトコルは、スマートカードの所有者を識別するときに、電話の時の携帯電話の使用の認証のときに、電子メールのメッセージの送り主が本物であることを確認するときなどの電子商取引においてきわめて重要なのです。

こういったことが確実にできる能力は、電子商取引の成功に特に大きく関わっています。

Further reading
参考文献

ハレルの本 Algorithmics には暗号化プロトコルに関連した電子署名について書いてあります。

そこには電話でポーカーをする方法についても紹介しています。その考え方は１９８１年 D.A. Klarner によって編集された The Mathematical Gardener の「メンタルポーカー」と呼ばれる章で取り上げられています。

Dorothy Denning の暗号化とデータセキュリティは暗号化に関するすぐれた情報科学の本です。

Dewdney の Turing Omnibus はこの学習の回路として使われた構成要素であるブール論理の章がある。