MT5462 Cipher Systems

Mark Wildon, mark.wildon@rhul.ac.uk

- **Sessions:**
  - Tuesday 1pm, **Plenary problem solving** (face-to-face) ARTS LT2,
  - Wednesday 12 noon, **Group work** (face-to-face), MFOX-SEM
  - Friday 10am, **Q&A session** (online)
  - Friday 3pm, **Group work** (online)

  Group work sessions **begin in Teaching Week 1**.
- **Extra session for MT5462:** Tuesday 11 am (Boiler 007).
- **Office hour McCrea LGF025 and online:** Thursday 2pm
- **Relevant seminars:** The Information Security Group Seminar is at 11am Thursdays. Of course it is now held online. To subscribe to the mailing list go to: www.lists.rhul.ac.uk/mailman/listinfo/isg-research-seminar. Later in term there will be Mathematics Seminars at 2pm Wednesday.

§1 Revision of fields and polynomials

Every modern cipher makes use of the finite field $\mathbb{F}_2$. Many use other finite fields as well: for example, a fundamental building block in AES (Advanced Encryption Standard) is the inversion map $x \mapsto x^{-1}$ on the non-zero elements of the finite field $\mathbb{F}_{2^8}$ with 256 elements.

Definition 1.1

A *field* is a set of elements $\mathbb{F}$ with two operations, $+$ (addition) and $\times$ (multiplication), and two special elements $0, 1 \in \mathbb{F}$ such that $0 \neq 1$ and

(1) $a + b = b + a$ for all $a, b \in \mathbb{F}$;
(2) $0 + a = a + 0 = a$ for all $a \in \mathbb{F}$;
(3) for all $a \in \mathbb{F}$ there exists $b \in \mathbb{F}$ such that $a + b = 0$;
(4) $a + (b + c) = (a + b) + c$ for all $a, b, c \in \mathbb{F}$;
(5) $a \times b = b \times a$ for all $a, b \in \mathbb{F}$;
(6) $1 \times a = a \times 1 = a$ for all $a \in \mathbb{F}$;
(7) for all non-zero $a \in \mathbb{F}$ there exists $b \in \mathbb{F}$ such that $a \times b = 1$;
(8) $a \times (b \times c) = (a \times b) \times c$ for all $a, b, c \in \mathbb{F}$;
(9) $a \times (b + c) = a \times b + a \times c$ for all $a, b, c \in \mathbb{F}$.

Basic Properties and Why $\mathbb{F}_p$ is a Field

Exercise 1.2

(a) Show, from the field axioms, that if $x \in \mathbb{F}$, then x has a unique additive inverse, and that if $x \neq 0$ then x has a unique multiplicative inverse. Show also that if $\mathbb{F}$ is a field then $a \times 0 = 0$ for all $a \in \mathbb{F}$.

(b) Show from the field axioms that if $\mathbb{F}$ is a field and a, $b \in \mathbb{F}$ are such that $ab = 0$, then either $a = 0$ or $b = 0$.

Theorem 1.3

Let p be a prime. The set $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ with addition and multiplication defined modulo p is a finite field of size p.

Quiz: What is the multiplicative inverse of 7 in the finite field $\mathbb{F}_{23}$? [*Hint:* use Euclid's Algorithm to solve $7q + 23s = 1$ and then read this equation modulo 23.]

(A) 3 (B) 7 (C) 10 (D) 17

Basic Properties and Why $\mathbb{F}_p$ is a Field

Exercise 1.2

(a) Show, from the field axioms, that if $x \in \mathbb{F}$, then x has a unique additive inverse, and that if $x \neq 0$ then x has a unique multiplicative inverse. Show also that if $\mathbb{F}$ is a field then $a \times 0 = 0$ for all $a \in \mathbb{F}$.

(b) Show from the field axioms that if $\mathbb{F}$ is a field and a, $b \in \mathbb{F}$ are such that $ab = 0$, then either $a = 0$ or $b = 0$.

Theorem 1.3

Let p be a prime. The set $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ with addition and multiplication defined modulo p is a finite field of size p.

Quiz: What is the multiplicative inverse of 7 in the finite field $\mathbb{F}_{23}$? [*Hint:* use Euclid's Algorithm to solve $7q + 23s = 1$ and then read this equation modulo 23.]

(A) 3 (B) 7 (C) 10 (D) 17

$\mathbb{F}_4$ is NOT the Integers Modulo 4

There is a unique (up to a suitable notion of isomorphism) finite field of any given prime-power size. The smallest field not of prime size is the finite field of size 4.

Example 1.4

The addition and multiplication tables for the finite field $\mathbb{F}_4 = \{0, 1, \alpha, 1+\alpha\}$ of size 4 are shown below.

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\times$	1	α	$1+\alpha$
1	1	α	$1+\alpha$
α	α	$1+\alpha$	1
$1+\alpha$	$1+\alpha$	1	α

Probably the most important thing to realise is that $\mathbb{F}_4$ **is not the integers modulo** 4. Indeed, in $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ we have $2 \times 2 = 0$, but if $a \in \mathbb{F}_4$ and $a \neq 0$ then $a \times a \neq 0$, as can be seen from the multiplication table. (Alternatively this follows from Exercise 1.2(b).)

Polynomials

Let $\mathbb{F}$ be a field. Let $\mathbb{F}[z]$ denote the set of all *polynomials*

$$f(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_m z^m$$

where $m \in \mathbb{N}_0$ and $a_0, a_1, a_2, \ldots, a_m \in \mathbb{F}$.

Definition 1.5

If $f(z) = a_0 + a_1 z + a_2 + \cdots + a_m z^m$ where $a_m \neq 0$, then we say that m is the *degree* of the polynomial f, and write $\deg f = m$. The degree of the zero polynomial is, by convention, -1. We say that a_0 is the *constant term* and a_m is the *leading term*.

Lemma 1.6 (Division of polynomials)

Let $\mathbb{F}$ be a field, let $g(z) \in \mathbb{F}[z]$ be a non-zero polynomial and let $f(z) \in \mathbb{F}[z]$. There exist polynomials $q(z), r(z) \in \mathbb{F}[z]$ such that

$$f(z) = q(z)g(z) + r(z)$$

and $\deg r(z) < \deg g(z)$.

Division of Polynomials

Lemma 1.6 (Division of polynomials)

Let $\mathbb{F}$ be a field, let $g(z) \in \mathbb{F}[z]$ be a non-zero polynomial and let $f(z) \in \mathbb{F}[z]$. There exist polynomials $q(z), r(z) \in \mathbb{F}[z]$ such that

$$f(z) = q(z)g(z) + r(z)$$

and $\deg r(z) < \deg g(z)$.

We say that $q(z)$ is the *quotient* and $r(z)$ is the *remainder* when $f(z)$ is divided by $g(z)$. Note that $r(z)$ may be zero, in which case its degree is -1. The important thing is that you can find the quotient and remainder in practice. In MATHEMATICA use

`PolynomialQuotientRemainder`

with `Modulus -> p` for the finite field $\mathbb{F}_p$ of prime size.

Division of Polynomials

Lemma 1.6 (Division of polynomials)

Let $\mathbb{F}$ be a field, let $g(z) \in \mathbb{F}[z]$ be a non-zero polynomial and let $f(z) \in \mathbb{F}[z]$. There exist polynomials $q(z), r(z) \in \mathbb{F}[z]$ such that

$$f(z) = q(z)g(z) + r(z)$$

and $\deg r(z) < \deg g(z)$.

Exercise 1.7

Let $g(z) = z^3 + z + 1 \in \mathbb{F}_2[z]$, let $f(z) = z^5 + z^2 + z \in \mathbb{F}_2[z]$.

(a) What is the quotient when $f(z)$ is divided by $g(z)$?

(A) $z^2 + 1$ (B) $z^2 + z + 1$ (C) $z + 1$ (D) $z^3 + z + 1$

(b) What is the remainder when $f(z)$ is divided by $g(z)$?

(A) 0 (B) 1 (C) $z + 1$ (D) $z^3 + z + 1$

(c) What is the remainder when $g(z)$ is divided by $f(z)$?

(A) $z^2 + 1$ (B) $z^2 + z + 1$ (C) $z + 1$ (D) $z^3 + z + 1$

Division of Polynomials

Lemma 1.6 (Division of polynomials)

Let $\mathbb{F}$ be a field, let $g(z) \in \mathbb{F}[z]$ be a non-zero polynomial and let $f(z) \in \mathbb{F}[z]$. There exist polynomials $q(z), r(z) \in \mathbb{F}[z]$ such that

$$f(z) = q(z)g(z) + r(z)$$

and $\deg r(z) < \deg g(z)$.

Exercise 1.7

Let $g(z) = z^3 + z + 1 \in \mathbb{F}_2[z]$, let $f(z) = z^5 + z^2 + z \in \mathbb{F}_2[z]$.

(a) What is the quotient when $f(z)$ is divided by $g(z)$?

(A) $z^2 + 1$ (B) $z^2 + z + 1$ (C) $z + 1$ (D) $z^3 + z + 1$

(b) What is the remainder when $f(z)$ is divided by $g(z)$?

(A) 0 (B) 1 (C) $z + 1$ (D) $z^3 + z + 1$

(c) What is the remainder when $g(z)$ is divided by $f(z)$?

(A) $z^2 + 1$ (B) $z^2 + z + 1$ (C) $z + 1$ (D) $z^3 + z + 1$

Division of Polynomials

Lemma 1.6 (Division of polynomials)

Let $\mathbb{F}$ be a field, let $g(z) \in \mathbb{F}[z]$ be a non-zero polynomial and let $f(z) \in \mathbb{F}[z]$. There exist polynomials $q(z), r(z) \in \mathbb{F}[z]$ such that

$$f(z) = q(z)g(z) + r(z)$$

and $\deg r(z) < \deg g(z)$.

Exercise 1.7

Let $g(z) = z^3 + z + 1 \in \mathbb{F}_2[z]$, let $f(z) = z^5 + z^2 + z \in \mathbb{F}_2[z]$.

(a) What is the quotient when $f(z)$ is divided by $g(z)$?

(A) $z^2 + 1$ (B) $z^2 + z + 1$ (C) $z + 1$ (D) $z^3 + z + 1$

(b) What is the remainder when $f(z)$ is divided by $g(z)$?

(A) 0 (B) 1 (C) $z + 1$ (D) $z^3 + z + 1$

(c) What is the remainder when $g(z)$ is divided by $f(z)$?

(A) $z^2 + 1$ (B) $z^2 + z + 1$ (C) $z + 1$ (D) $z^3 + z + 1$

Division of Polynomials

Lemma 1.6 (Division of polynomials)

Let $\mathbb{F}$ be a field, let $g(z) \in \mathbb{F}[z]$ be a non-zero polynomial and let $f(z) \in \mathbb{F}[z]$. There exist polynomials $q(z), r(z) \in \mathbb{F}[z]$ such that

$$f(z) = q(z)g(z) + r(z)$$

and $\deg r(z) < \deg g(z)$.

Exercise 1.7

Let $g(z) = z^3 + z + 1 \in \mathbb{F}_2[z]$, let $f(z) = z^5 + z^2 + z \in \mathbb{F}_2[z]$.

(a) What is the quotient when $f(z)$ is divided by $g(z)$?

(A) $z^2 + 1$ (B) $z^2 + z + 1$ (C) $z + 1$ (D) $z^3 + z + 1$

(b) What is the remainder when $f(z)$ is divided by $g(z)$?

(A) 0 (B) 1 (C) $z + 1$ (D) $z^3 + z + 1$

(c) What is the remainder when $g(z)$ is divided by $f(z)$?

(A) $z^2 + 1$ (B) $z^2 + z + 1$ (C) $z + 1$ (D) $z^3 + z + 1$

Polynomials and Roots

Lemma 1.8

Let $\mathbb{F}$ be a field.

(i) *If $f(z) \in \mathbb{F}[z]$ has $a \in \mathbb{F}$ as a root, i.e. $f(a) = 0$, then there is a polynomial $q(z) \in \mathbb{F}[z]$ such that $f(z) = (z - a)q(z)$.*

(ii) *If $f(z) \in \mathbb{F}[z]$ has degree $m \in \mathbb{N}_0$ then $f(z)$ has at most m distinct roots in $\mathbb{F}$.*

(iii) *Suppose that $f(z)$, $g(z) \in \mathbb{F}[z]$ are non-zero polynomials such that $\deg f$, $\deg g < t$. If there exist distinct $c_1, \ldots, c_t \in \mathbb{F}$ such that $f(c_i) = g(c_i)$ for each $i \in \{1, \ldots, t\}$ then $f(z) = g(z)$.*

Quiz: Work in the finite field $\mathbb{F}_3$ in which $2 + 1 = 0$ and $2 \times 2 = 1$. Let $f(z) = z^3 + z^2 - z - 1 \in \mathbb{F}_3[z]$.

(a) What is the polynomial $q(z)$ when the root is 1?

(A) $z^2 - z + 1$ (B) $z^2 - 1$ (C) $z - 1$ (D) does not exist

(b) How many distinct roots does $f(z)$ have in $\mathbb{F}_3[z]$?

(A) 1 (B) 2 (C) 3 (D) 4

Polynomials and Roots

Lemma 1.8

Let $\mathbb{F}$ be a field.

(i) *If $f(z) \in \mathbb{F}[z]$ has $a \in \mathbb{F}$ as a root, i.e. $f(a) = 0$, then there is a polynomial $q(z) \in \mathbb{F}[z]$ such that $f(z) = (z - a)q(z)$.*

(ii) *If $f(z) \in \mathbb{F}[z]$ has degree $m \in \mathbb{N}_0$ then $f(z)$ has at most m distinct roots in $\mathbb{F}$.*

(iii) *Suppose that $f(z)$, $g(z) \in \mathbb{F}[z]$ are non-zero polynomials such that $\deg f$, $\deg g < t$. If there exist distinct $c_1, \ldots, c_t \in \mathbb{F}$ such that $f(c_i) = g(c_i)$ for each $i \in \{1, \ldots, t\}$ then $f(z) = g(z)$.*

Quiz: Work in the finite field $\mathbb{F}_3$ in which $2 + 1 = 0$ and $2 \times 2 = 1$.
Let $f(z) = z^3 + z^2 - z - 1 \in \mathbb{F}_3[z]$.

(a) What is the polynomial $q(z)$ when the root is 1?

(A) $z^2 - z + 1$ (B) $z^2 - 1$ (C) $z - 1$ (D) does not exist

(b) How many distinct roots does $f(z)$ have in $\mathbb{F}_3[z]$?

(A) 1 (B) 2 (C) 3 (D) 4

Polynomials and Roots

Lemma 1.8

Let $\mathbb{F}$ be a field.

(i) *If $f(z) \in \mathbb{F}[z]$ has $a \in \mathbb{F}$ as a root, i.e. $f(a) = 0$, then there is a polynomial $q(z) \in \mathbb{F}[z]$ such that $f(z) = (z - a)q(z)$.*

(ii) *If $f(z) \in \mathbb{F}[z]$ has degree $m \in \mathbb{N}_0$ then $f(z)$ has at most m distinct roots in $\mathbb{F}$.*

(iii) *Suppose that $f(z)$, $g(z) \in \mathbb{F}[z]$ are non-zero polynomials such that $\deg f$, $\deg g < t$. If there exist distinct $c_1, \ldots, c_t \in \mathbb{F}$ such that $f(c_i) = g(c_i)$ for each $i \in \{1, \ldots, t\}$ then $f(z) = g(z)$.*

Quiz: Work in the finite field $\mathbb{F}_3$ in which $2 + 1 = 0$ and $2 \times 2 = 1$.
Let $f(z) = z^3 + z^2 - z - 1 \in \mathbb{F}_3[z]$.

(a) What is the polynomial $q(z)$ when the root is 1?

(A) $z^2 - z + 1$ (B) $z^2 - 1$ (C) $z - 1$ (D) does not exist

(b) How many distinct roots does $f(z)$ have in $\mathbb{F}_3[z]$?

(A) 1 (B) 2 (C) 3 (D) 4

Polynomials and Roots

Lemma 1.8

Let $\mathbb{F}$ be a field.

(i) *If $f(z) \in \mathbb{F}[z]$ has $a \in \mathbb{F}$ as a root, i.e. $f(a) = 0$, then there is a polynomial $q(z) \in \mathbb{F}[z]$ such that $f(z) = (z - a)q(z)$.*

(ii) *If $f(z) \in \mathbb{F}[z]$ has degree $m \in \mathbb{N}_0$ then $f(z)$ has at most m distinct roots in $\mathbb{F}$.*

(iii) *Suppose that $f(z)$, $g(z) \in \mathbb{F}[z]$ are non-zero polynomials such that $\deg f$, $\deg g < t$. If there exist distinct $c_1, \ldots, c_t \in \mathbb{F}$ such that $f(c_i) = g(c_i)$ for each $i \in \{1, \ldots, t\}$ then $f(z) = g(z)$.*

Part (iii) is the critical result. It says, for instance, that a linear polynomial is determined by two points on its graph: when $\mathbb{F}$ is the real numbers $\mathbb{R}$ this should be intuitive — there is a unique line through any two distinct points. Similarly a quadratic is determined by any three points on its graph, and so on.

Polynomial Interpolation

Conversely, given t values in a field $\mathbb{F}$, there is a polynomial in $\mathbb{F}[z]$ of degree at most t taking these values at any t distinct specified points. This has a nice constructive proof.

Lemma 1.9 (Polynomial interpolation)

Let $\mathbb{F}$ be a field. Let

$$c_1, c_2, \ldots, c_t \in \mathbb{F}$$

be distinct and let $y_1, y_2, \ldots, y_t \in \mathbb{F}$. The unique polynomial $f(z) \in \mathbb{F}[z]$, either zero or of degree $< t$, such that $f(c_i) = y_i$ for all i is

$$f(z) = \sum_{i=1}^{t} y_i \frac{\prod_{j \neq i}(z - c_j)}{\prod_{j \neq i}(c_i - c_j)}.$$

Later we shall use polynomials in multiple variables with coefficients in $\mathbb{F}_2$ to describe cryptographic primitives.

§2: Shamir's Secret Sharing Scheme

As a standing convention, we write secret information in red. This is entirely optional for you and not standard.

Example 2.1

Ten people want to know their mean salary. But none is willing to reveal her salary s_i to the others, or to a 'Trusted Third Party'. Instead Person 1 chooses a large number M. She remembers M, and whispers $M + s_1$ to Person 2. Then Person 2 whispers $M + s_1 + s_2$ to Person 3, and so on, until Person 10 whispers $M + s_1 + s_2 + \cdots + s_9 + s_{10}$ to Person 1. Person 1 then subtracts M and tells everyone the mean $(s_1 + s_2 + \cdots + s_{10})/10$.

Exercise 2.2

Why it is reasonable to colour code the whisper from Person 2 as $M + s_1 + s_2$, with $M + s_1$ all in red?

Secret Sharing Salaries: No Information Leak

Exercise 2.3

Show that if Person j hears N from Person $j-1$ then $s_1 + \cdots + s_{j-1}$ can consistently be any number between 0 and N.

Exercise 2.4

Person 1 can deduce the total of the salaries of all the other people from $M + s_1 + \cdots + s_n$ by subtracting $M + s_1$. In particular, if $n = 2$, she can learn Person 2's salary. Is this a defect in the scheme?

Shamir Secret Sharing Scheme

Definition 2.5

Let p be a prime and let $s \in \mathbb{F}_p$. Let $n \in \mathbb{N}$, $t \in \mathbb{N}$ be such that $t \leq n < p$. Let $c_1, \ldots, c_n \in \mathbb{F}_p$ be distinct non-zero elements. In the *Shamir scheme* with n people and *threshold* t, to share the secret $s \in \mathbb{F}_p$, Trevor chooses at random $a_1, \ldots, a_{t-1} \in \mathbb{F}_p$ and constructs the polynomial

$$f(x) = s + a_1 z + \cdots + a_{t-1} z^{t-1}$$

with constant term s. Trevor then issues the *share* $f(c_i)$ to Person i.

As often the case in cryptography, it is important to be clear about what is private and what is public.

Above we wrote $f(c_i)$ because the evaluation points c_i are public knowledge, as are the parameters n, t and p. Only Trevor knows $f(z)$, and at the time it is issued, the share $f(c_i)$ (written all in red, as it's secret) is known only to Person i and Trevor.

Shamir Secret Sharing Scheme: Example

Example 2.6

Suppose that $n = 5$ and $t = 3$. Take $p = 7$ and $c_i = i$ for each $i \in \{1, 2, 3, 4, 5\}$. We suppose that $s = 5$. Trevor chooses $a_1, a_2 \in \mathbb{F}_7$ at random, getting $a_1 = 6$ and $a_2 = 1$. Therefore $f(z) = 5 + 6z + 1z^2$ and the share of Person i is $f(c_i)$, for each $i \in \{1, 2, 3, 4, 5\}$, so the shares for each person are

$$\big(f(1), f(2), f(3), f(4), f(5)\big) = (5, 0, 4, 3, 4).$$

Remember that all arithmetic is performed in $\mathbb{F}_p$, so working modulo p.

Shamir Secret Sharing Scheme: No Information Leak

The following exercise shows the main idea needed to prove Theorem 2.8 below.

Exercise 2.7

Suppose that Person 1, with share $f(1) = 5$, and Person 2, with share $f(2) = 0$, cooperate in an attempt to discover s. Show that for each $s' \in \mathbb{F}_7$ there exists a unique polynomial $f_{s'}(z)$ such that $\deg f \leq 2$ and $f(0) = s'$, $f_z(1) = 5$ and $f_z(2) = 0$. For example $f_2(z) = 3z^2 + 2$ and $f_3(z) = 2z + 3$. Since Trevor chose the coefficients of f at random, each polynomial $f_0(z), \ldots, f_{p-1}(z)$ seems equally likely to Persons 1 and 2, and they can learn nothing about s.

Theorem 2.8

In a Shamir scheme with n people, threshold t and secret s, any t people can work together to determine s but any $t-1$ people, even if they work together, can learn nothing about s.

Pre-requisites for Proof of Theorem 2.8

Lemma 1.8

Let $\mathbb{F}$ be a field.

(iii) *Suppose that $f(z), g(z) \in \mathbb{F}[z]$ are non-zero polynomials such that $\deg f, \deg g < t$. If there exist distinct $c_1, \ldots, c_t \in \mathbb{F}$ such that $f(c_i) = g(c_i)$ for each $i \in \{1, \ldots, t\}$ then $f(z) = g(z)$.*

Lemma 1.9 (Polynomial interpolation)

Let $\mathbb{F}$ be a field. Let $c_1, c_2, \ldots, c_t \in \mathbb{F}$ be distinct and let $y_1, y_2, \ldots, y_t \in \mathbb{F}$. The unique polynomial $f(z) \in \mathbb{F}[z]$, either zero or of degree $< t$, such that $f(c_i) = y_i$ for all i is

$$f(z) = \sum_{i=1}^{t} y_i \frac{\prod_{j \neq i}(z - c_j)}{\prod_{j \neq i}(c_i - c_j)}.$$

Adversarial Secret Sharing

Exercise 2.9

Suppose Trevor shares $s \in \mathbb{F}_p$ across n computers using the Shamir scheme with threshold t. He chooses the first t computers. They are instructed to exchange their shares; then each computes s and sends it to Trevor. Unfortunately Malcolm has compromised computer 1. Show that Malcolm can both learn s and trick Trevor into thinking his secret is an $s' \in \mathbb{F}_p$ of his choice.

(Assume that, thanks to a network delays, it is plausible that computer 1 sends its share after receiving the shares from the other $t - 1$ computers.)

Shamir's Secret Sharing Scheme has been modified in various ways to get around this problem. See Martin Tompa and Heather Woll, *How to share a secret with cheaters*, J. Crypt. **1** (1989) 133–138 for an introduction.

Addition and Multiplication in the Cloud

Exercise 2.10

Take the Shamir scheme with threshold t and evaluation points $1, \ldots, n \in \mathbb{F}_p$ where $p > n$. Trevor has shared two large numbers r and s across n cloud computers, using polynomials f and g so that the shares are $\big(f(1), \ldots, f(n)\big)$ and $\big(g(1), \ldots, g(n)\big)$.

(a) Express in terms of f and g a polynomial suitable for sharing the secret $s + t$. [*Hint:* this will seem obvious in hindsight, but is easily missed.]

(b) Imagine you are Cloud Computer 1, so you know the shares $f(c_1)$ for r and $g(c_1)$ for s. What is your share for $s + t$, using the polynomial from (a)? Can you compute this share yourself?

(c) Show that the n computers can each compute the shares for $s + t$ without exchanging any information.

(d) (**Optional extension.**) Assume that $n \geq 2t$. Show that the cloud computers can compute shares for rs mod p sending information only between each other.

Optional Extras on Secret Sharing: DNSSEC

Example 2.11

The root key for DNSSEC, part of web of trust that guarantees an IP connection really is to the claimed end-point, and not Malcolm doing a Man-in-the-Middle attack, is protected by a secret sharing scheme with $n = 7$ and $t = 5$: search for 'Schneier DNSSEC'.

The search above will take you to Bruce Schneier's blog. It is highly recommended for background on practical cryptography.

Optional Extras on Secret Sharing: Reed–Solomon Codes

Remark 2.12

The Reed–Solomon code associated to the parameters p, n, t and the field elements $c_1, c_2, \ldots, c_n$ is the length n code over $\mathbb{F}_p$ with codewords all possible n-tuples

$$\{\big(f(c_1), f(c_2), \ldots, f(c_n)\big) : f \in \mathbb{F}_p[z],\ \deg f \leq t-1\}.$$

It will be studied in MT5461. By Theorem 2.8, each codeword is determined by any t of its positions, and so two codewords agreeing in t positions are equal. This shows that any two different codewords differ in at least $n-(t-1)$ positions. Equivalently, the Reed–Solomon code has minimum distance at least $n-t+1$.

Optional Extras on Secret Sharing: Reed–Solomon Codes

Remark 2.12

The Reed–Solomon code associated to the parameters p, n, t and the field elements $c_1, c_2, \ldots, c_n$ is the length n code over $\mathbb{F}_p$ with codewords all possible n-tuples

$$\{\big(f(c_1), f(c_2), \ldots, f(c_n)\big) : f \in \mathbb{F}_p[z],\ \deg f \leq t-1\}.$$

It will be studied in MT5461. By Theorem 2.8, each codeword is determined by any t of its positions, and so two codewords agreeing in t positions are equal. This shows that any two different codewords differ in at least $n-(t-1)$ positions. Equivalently, the Reed–Solomon code has minimum distance at least $n-t+1$.

For simplicity we have worked over a finite field of prime size in this section. Reed–Solomon codes and the Shamir secret sharing scheme generalize in the obvious way to arbitrary finite fields. For example, the Reed–Solomon codes used on compact discs have alphabet the finite field $\mathbb{F}_{2^8}$.

§3 Introduction to boolean Functions

Recall that $\mathbb{F}_2 = \{0, 1\}$ is the finite field of size 2 whose elements are the *bits* 0 and 1. As usual, $+$ denotes addition in $\mathbb{F}_2$ or in $\mathbb{F}_2^n$. We number positions in $\mathbb{F}_2^n$ from 0, so a typical tuple is $(x_0, x_1, \ldots, x_{n-1})$.

Definition 3.1

Let $n \in \mathbb{N}$. An n-variable *boolean function* is a function $\mathbb{F}_2^n \to \mathbb{F}_2$.

For example, $f(x, y, z) = xyz + x$ is a boolean function of the three variables x, y and z, such that $f(1, 0, 0) = 0 + 1 = 1$ and $f(1, 1, 1) = 1 + 1 = 0$. We shall see that boolean functions are very useful for describing the primitive building blocks of modern stream and block ciphers.

Exercise 3.2

What is a simpler form for $x^2y + xz + z + z^2$?

Almost the Smallest Interesting Non-Linear Function?

Exercise 3.3

Let $\mathrm{maj}(x, y, z) = xy + yz + zx$ where, as usual, the coefficients are in $\mathbb{F}_2$. Show that

$$\mathrm{maj}(x, y, z) = \begin{cases} 0 & \text{if at most one of } x, y, z \text{ is } 1 \\ 1 & \text{if at least two of } x, y, z \text{ are } 1. \end{cases}$$

We call $\mathrm{maj} : \mathbb{F}_2^3 \to \mathbb{F}_2$ the *majority vote function*. It is a 3-variable boolean function.

Block Ciphers

A block cipher has plaintexts and ciphertexts $\mathbb{F}_2^n$ for some fixed n. The encryption functions are typically defined by composing carefully chosen cryptographic primitives over a number of *rounds*.

Example 3.4

(1) Each round of the widely used block cipher AES is of the form $(x, k) \mapsto s(x) + k$ where $+$ is addition in $\mathbb{F}_2^{128}$, $x \in \mathbb{F}_2^{128}$ is the input to the round (derived ultimately from the plaintext) and $k \in \mathbb{F}_2^{128}$ is a 'round key' derived from the key.

The most important cryptographic primitive in the function $s : \mathbb{F}_2^{128} \to \mathbb{F}_2^{128}$ is inversion in the finite field $\mathbb{F}_{2^8}$. The inversion function is highly non-linear and hard to attack. Just for fun, the 255 values of the boolean function sending 0 to 0 and a non-zero x to the bit in position 0 of x^{-1} are shown below, for one natural order on $\mathbb{F}_{2^8}$.

$$
\begin{array}{l}
01101011011001110001110101101000000111011001000001001100010111111 \\
10111111101101111010001100001011001110010111111111110100000010 \\
10100100101110100001000000101010100110100000010000111101100110 \\
10110001111010000101110001011001110100110011100111000010101010.
\end{array}
$$

SPECK

(2) In the block cipher SPECK proposed by NSA in June 2013, the non-linear primitive is modular addition in $\mathbb{Z}/2^m\mathbb{Z}$. As a 'toy' version we take $m = 8$; in practice m is at least 16 and usually 64. Identify $\mathbb{F}_2^8$ with $\mathbb{Z}/2^8\mathbb{Z}$ by writing numbers in their binary form. For instance, $13 \in \mathbb{Z}/2^8\mathbb{Z}$ has binary form 0000 1101 (the space is just for readability) and

$$1010\,1010 \boxplus 0000\,1111 = 1011\,1001$$
$$1000\,0001 \boxplus 1000\,0001 = 0000\,0010$$

corresponding to $170 + 15 = 185 \bmod 256$ and $129 + 129 = 2 \bmod 256$. Modular addition is a convenient operation because it is very fast on a computer, but it has some cryptographic weaknesses. In SPECK it is combined with other functions in a way that appears to give a very strong and fast cipher.

Modular Addition as a boolean Function

One sign that modular addition is weak is that the low numbered bits are 'close to' linear functions. We make this precise in §6 on linear cryptanalysis. For example

$$\begin{aligned}(\ldots, x_2, x_1, x_0) \boxplus (\ldots, y_2, y_1, y_0) \\ = (\ldots, x_2 + y_2 + c_2, x_1 + y_1 + x_0 y_0, x_0 + y_0)\end{aligned}$$

where c_2 is the carry into position 2, defined using the majority vote function by $c_2 = \mathrm{maj}(x_1, y_1, x_0 y_0)$. Unless both x_0 and y_0 are 1, bit 1 is $x_1 + y_1$, a linear function of $(\ldots, x_2, x_1, x_0)$ and $(\ldots, y_2, y_1, y_0)$. By Exercise 4.5, output bit 2 is given by the more complicated polynomial

$$x_2 + y_2 + x_1 y_1 + x_0 x_1 y_0 + x_0 y_0 y_1.$$

This formula can be used for part of Question 6 on Problem Sheet 2: it is the algebraic normal form of the boolean function for bit 2 in modular addition.

Quiz on Binary Form and $\boxplus$ modulo 2^4

- What is the 4-bit binary form of 11?

  (A) 1101 (B) 1011 (C) 0111 (D) 1001

- What is the 4-bit binary form of 7?

  (A) 0011 (B) 0111 (C) 1011 (D) 1101

- In the previous slide we saw that output bit 1 of $x \boxplus y$ is given by $x_1 + y_1 + x_0 y_0$ and output bit 2 of $x + y$ is given by

  $$x_2 + y_2 + x_1 y_1 + x_0 x_1 y_0 + x_0 y_0 y_1.$$

  According to these formulae, what is $11 \boxplus 7$?

  (A) ?00? (B) ?01? (C) ?10? (D) ?11?

- What is the formula for output bit 0 of $x \boxplus y$?

  (A) $x_0 + y_0$ (B) $x_0 + y_0 + x_0 y_0$ (C) $x_0 + x_1$ (D) other

- What is the 4-bit binary form of $11 \boxplus 7$?

  (A) 0010 (B) 1010 (C) 1000 (D) 1110

- To think about: what is special about output bit 0 compared to the other bits?

Quiz on Binary Form and $\boxplus$ modulo 2^4

- What is the 4-bit binary form of 11?

  (A) 1101 (B) 1011 (C) 0111 (D) 1001

- What is the 4-bit binary form of 7?

  (A) 0011 (B) 0111 (C) 1011 (D) 1101

- In the previous slide we saw that output bit 1 of $x \boxplus y$ is given by $x_1 + y_1 + x_0 y_0$ and output bit 2 of $x + y$ is given by

  $$x_2 + y_2 + x_1 y_1 + x_0 x_1 y_0 + x_0 y_0 y_1.$$

  According to these formulae, what is $11 \boxplus 7$?

  (A) ?00? (B) ?01? (C) ?10? (D) ?11?

- What is the formula for output bit 0 of $x \boxplus y$?

  (A) $x_0 + y_0$ (B) $x_0 + y_0 + x_0 y_0$ (C) $x_0 + x_1$ (D) other

- What is the 4-bit binary form of $11 \boxplus 7$?

  (A) 0010 (B) 1010 (C) 1000 (D) 1110

- To think about: what is special about output bit 0 compared to the other bits?

Quiz on Binary Form and $\boxplus$ modulo 2^4

- What is the 4-bit binary form of 11?

  (A) 1101 (B) 1011 (C) 0111 (D) 1001

- What is the 4-bit binary form of 7?

  (A) 0011 (B) 0111 (C) 1011 (D) 1101

- In the previous slide we saw that output bit 1 of $x \boxplus y$ is given by $x_1 + y_1 + x_0 y_0$ and output bit 2 of $x + y$ is given by

  $$x_2 + y_2 + x_1 y_1 + x_0 x_1 y_0 + x_0 y_0 y_1.$$

  According to these formulae, what is $11 \boxplus 7$?

  (A) ?00? (B) ?01? (C) ?10? (D) ?11?

- What is the formula for output bit 0 of $x \boxplus y$?

  (A) $x_0 + y_0$ (B) $x_0 + y_0 + x_0 y_0$ (C) $x_0 + x_1$ (D) other

- What is the 4-bit binary form of $11 \boxplus 7$?

  (A) 0010 (B) 1010 (C) 1000 (D) 1110

- To think about: what is special about output bit 0 compared to the other bits?

Quiz on Binary Form and $\boxplus$ modulo 2^4

- What is the 4-bit binary form of 11?

  (A) 1101 (B) 1011 (C) 0111 (D) 1001

- What is the 4-bit binary form of 7?

  (A) 0011 (B) 0111 (C) 1011 (D) 1101

- In the previous slide we saw that output bit 1 of $x \boxplus y$ is given by $x_1 + y_1 + x_0 y_0$ and output bit 2 of $x + y$ is given by

  $$x_2 + y_2 + x_1 y_1 + x_0 x_1 y_0 + x_0 y_0 y_1.$$

  According to these formulae, what is $11 \boxplus 7$?

  (A) ?00? (B) ?01? (C) ?10? (D) ?11?

- What is the formula for output bit 0 of $x \boxplus y$?

  (A) $x_0 + y_0$ (B) $x_0 + y_0 + x_0 y_0$ (C) $x_0 + x_1$ (D) other

- What is the 4-bit binary form of $11 \boxplus 7$?

  (A) 0010 (B) 1010 (C) 1000 (D) 1110

- To think about: what is special about output bit 0 compared to the other bits?

Quiz on Binary Form and $\boxplus$ modulo 2^4

- What is the 4-bit binary form of 11?

  (A) 1101 (B) 1011 (C) 0111 (D) 1001

- What is the 4-bit binary form of 7?

  (A) 0011 (B) 0111 (C) 1011 (D) 1101

- In the previous slide we saw that output bit 1 of $x \boxplus y$ is given by $x_1 + y_1 + x_0 y_0$ and output bit 2 of $x + y$ is given by

  $$x_2 + y_2 + x_1 y_1 + x_0 x_1 y_0 + x_0 y_0 y_1.$$

  According to these formulae, what is $11 \boxplus 7$?

  (A) ?00? (B) ?01? (C) ?10? (D) ?11?

- What is the formula for output bit 0 of $x \boxplus y$?

  (A) $x_0 + y_0$ (B) $x_0 + y_0 + x_0 y_0$ (C) $x_0 + x_1$ (D) other

- What is the 4-bit binary form of $11 \boxplus 7$?

  (A) 0010 (B) 1010 (C) 1000 (D) 1110

- To think about: what is special about output bit 0 compared to the other bits?

Quiz on Binary Form and $\boxplus$ modulo 2^4

- What is the 4-bit binary form of 11?

  (A) 1101 (B) 1011 (C) 0111 (D) 1001

- What is the 4-bit binary form of 7?

  (A) 0011 (B) 0111 (C) 1011 (D) 1101

- In the previous slide we saw that output bit 1 of $x \boxplus y$ is given by $x_1 + y_1 + x_0 y_0$ and output bit 2 of $x + y$ is given by

  $$x_2 + y_2 + x_1 y_1 + x_0 x_1 y_0 + x_0 y_0 y_1.$$

  According to these formulae, what is $11 \boxplus 7$?

  (A) ?00? (B) ?01? (C) ?10? (D) ?11?

- What is the formula for output bit 0 of $x \boxplus y$?

  (A) $x_0 + y_0$ (B) $x_0 + y_0 + x_0 y_0$ (C) $x_0 + x_1$ (D) other

- What is the 4-bit binary form of $11 \boxplus 7$?

  (A) 0010 (B) 1010 (C) 1000 (D) 1110

- To think about: what is special about output bit 0 compared to the other bits?

Truth Tables and Disjunctive Normal Form

A boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be defined by its *truth table*, which records for each $x \in \mathbb{F}_2^n$ its image $f(x)$. For example, the boolean functions $\mathbb{F}_2^2 \to \mathbb{F}_2$ of addition and multiplication are shown below:

x	y	$x+y$	xy	$x \wedge y$	$x \vee y$	$x \implies y$
0	0	0	0	F	F	
0	1	1	0	F	T	
1	0	1	0	F	T	
1	1	0	1	T	T	

It is often useful to think of 0 as false and 1 as true. Then xy corresponds to $x \wedge y$, the logical 'and' of x and y, as shown above. The logical 'or' of x and y is denoted $x \vee y$.

Truth Tables and Disjunctive Normal Form

A boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be defined by its *truth table*, which records for each $x \in \mathbb{F}_2^n$ its image $f(x)$. For example, the boolean functions $\mathbb{F}_2^2 \to \mathbb{F}_2$ of addition and multiplication are shown below:

x	y	$x+y$	xy	$x \wedge y$	$x \vee y$	$x \implies y$
0	0	0	0	F	F	
0	1	1	0	F	T	
1	0	1	0	F	T	
1	1	0	1	T	T	

It is often useful to think of 0 as false and 1 as true. Then xy corresponds to $x \wedge y$, the logical 'and' of x and y, as shown above. The logical 'or' of x and y is denoted $x \vee y$.

Exercise 3.5

Use the true/false interpretation to complete the columns for $x \implies y$. Could you convince a sceptical friend that false statement imply true statements?

Toffoli Function

Example 3.6

The Toffoli function is a 3-variable boolean function important in quantum computing. It can be defined by

$$\text{toffoli}(x_0, x_1, x_2) = \begin{cases} x_0 & \text{if } x_1 x_2 = 0 \\ \overline{x_0} & \text{if } x_1 x_2 = 1. \end{cases}$$

Here $\overline{x}$ denotes the bitflip of x, defined by $\overline{0} = 1$ and $\overline{1} = 0$. In the true/false interpretation $\overline{F} = T$ and $\overline{T} = F$.

	x_2	x_1	x_0	$\text{maj}(x_0, x_1, x_2)$	$\text{toffoli}(x_0, x_1, x_2)$	$f_{\{0\}}$	$f_{\{0,2\}}$
$\varnothing$	0	0	0	0	0	0	0
$\{0\}$	0	0	1	0	1	1	0
$\{1\}$	0	1	0	0	0	0	0
$\{0,1\}$	0	1	1	1	1	0	0
$\{2\}$	1	0	0	0	0	0	0
$\{0,2\}$	1	0	1	1	1	0	1
$\{1,2\}$	1	1	0	1	1	0	0
$\{0,1,2\}$	1	1	1	1	0	0	0

A Step Towards Disjunctive Normal Form for Toffoli

	x_2	x_1	x_0	$\mathrm{maj}(x_0, x_1, x_2)$	$\mathrm{toffoli}(x_0, x_1, x_2)$	$f_{\{0\}}$	$f_{\{0,2\}}$
$\varnothing$	0	0	0	0	0	0	0
$\{0\}$	0	0	1	0	1	1	0
$\{1\}$	0	1	0	0	0	0	0
$\{0,1\}$	0	1	1	1	1	0	0
$\{2\}$	1	0	0	0	0	0	0
$\{0,2\}$	1	0	1	1	1	0	1
$\{1,2\}$	1	1	0	1	1	0	0
$\{0,1,2\}$	1	1	1	1	0	0	0

The sets on the left record which variables are true. For example, the majority vote function is true on the rows labelled by the sets of sizes 2 and 3, namely, $\{0,1\}, \{0,2\}, \{1,2\}, \{1,2,3\}$, and false on the other rows.

Disjunctive Normal Form: Motivation

Given a subset J of $\{0, \ldots, n-1\}$ we define $f_J : \mathbb{F}_2^n \to \mathbb{F}_2$ by

$$f_J(x) = \bigwedge_{j \in J} x_j \wedge \bigwedge_{j \notin J} \overline{x}_j.$$

In words, f_J is the n-variable boolean function whose truth table has a unique 1 (or true) in the row labelled J. For instance $f_{\{0\}}(x_0, x_1, x_2) = x_0 \wedge \overline{x}_1 \wedge \overline{x}_2$ and $f_{\{0,2\}}(x_0, x_1, x_2) = x_0 \wedge \overline{x}_1 \wedge x_2$ are on the previous slide.

Exercise 3.7

(i) For what set J do we have

$$\text{toffoli} = f_{\{0\}} \vee f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_J?$$

(ii) Express the majority vote function in the form above.

(iii) Find a way to complete the right-hand side in

$$\text{maj}(x) = (x_0 \wedge x_1 \wedge \overline{x}_2) \vee (x_0 \wedge \overline{x}_1 \wedge x_2) \vee (\overline{x}_0 \wedge x_1 \wedge x_2) \vee (\ldots).$$

This should seem almost the same as (ii).

Disjunctive Normal Form: Motivation

Recall that $f_J(x) = \bigwedge_{j \in J} x_j \wedge \bigwedge_{j \notin J} \overline{x}_j$. It is defined so that

$$f_J(x) = 1 \text{ if and only if } x_j = 1 \iff j \in J.$$

	x_2	x_1	x_0	$\mathrm{maj}(x_0, x_1, x_2)$	$\mathrm{toffoli}(x_0, x_1, x_2)$	$f_{\{0\}}$	$f_{\{0,2\}}$	True
$\varnothing$	0	0	0	0	0	0	0	1
$\{0\}$	0	0	1	0	1	1	0	1
$\{1\}$	0	1	0	0	0	0	0	1
$\{0,1\}$	0	1	1	1	1	0	0	1
$\{2\}$	1	0	0	0	0	0	0	1
$\{0,2\}$	1	0	1	1	1	0	1	1
$\{1,2\}$	1	1	0	1	1	0	0	1
$\{0,1,2\}$	1	1	1	1	0	0	0	1

We saw in Exercise 3.7 that

(a) $\mathrm{toffoli} = f_{\{0\}} \vee f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}}$;

(b) $\mathrm{maj} = f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}} \vee f_{\{0,1,2\}}$; equivalently,

$$\mathrm{maj}(x_0, x_1, x_2) = (x_0 \wedge x_1 \wedge \overline{x}_2) \vee (x_0 \wedge \overline{x}_1 \wedge x_2) \vee (\overline{x}_0 \wedge x_1 \wedge x_2) \vee (x_0 \wedge x_1 \wedge x_2).$$

How would you express the boolean function $g(x_0, x_1, x_2)$ that is true if and only if $x_0 = x_1 = x_2$ as a disjunction ($\bigvee$) of the f_J?

Disjunctive Normal Form: Motivation

Recall that $f_J(x) = \bigwedge_{j \in J} x_j \wedge \bigwedge_{j \notin J} \overline{x}_j$. It is defined so that

$$f_J(x) = 1 \text{ if and only if } x_j = 1 \iff j \in J.$$

	x_2	x_1	x_0	$\mathrm{maj}(x_0, x_1, x_2)$	$\mathrm{toffoli}(x_0, x_1, x_2)$	$f_{\{0\}}$	$f_{\{0,2\}}$	True
$\varnothing$	0	0	0	0	0	0	0	1
$\{0\}$	0	0	1	0	1	1	0	1
$\{1\}$	0	1	0	0	0	0	0	1
$\{0,1\}$	0	1	1	1	1	0	0	1
$\{2\}$	1	0	0	0	0	0	0	1
$\{0,2\}$	1	0	1	1	1	0	1	1
$\{1,2\}$	1	1	0	1	1	0	0	1
$\{0,1,2\}$	1	1	1	1	0	0	0	1

We saw in Exercise 3.7 that

(a) $\mathrm{toffoli} = f_{\{0\}} \vee f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}}$;

(b) $\mathrm{maj} = f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}} \vee f_{\{0,1,2\}}$; equivalently,

$$\mathrm{maj}(x_0, x_1, x_2) = (x_0 \wedge x_1 \wedge \overline{x}_2) \vee (x_0 \wedge \overline{x}_1 \wedge x_2) \vee (\overline{x}_0 \wedge x_1 \wedge x_2) \vee (x_0 \wedge x_1 \wedge x_2).$$

How would you express the boolean function $g(x_0, x_1, x_2)$ that is true if and only if $x_0 = x_1 = x_2$ as a disjunction $(\bigvee)$ of the f_J?

Answer. It's simply $x_0 \wedge x_1 \wedge x_2$ with just one '$\vee$ clause'.

Disjunctive Normal Form: Motivation

Recall that $f_J(x) = \bigwedge_{j \in J} x_j \wedge \bigwedge_{j \notin J} \overline{x}_j$. It is defined so that

$$f_J(x) = 1 \text{ if and only if } x_j = 1 \iff j \in J.$$

	x_2	x_1	x_0	$\mathrm{maj}(x_0, x_1, x_2)$	$\mathrm{toffoli}(x_0, x_1, x_2)$	$f_{\{0\}}$	$f_{\{0,2\}}$	True
$\varnothing$	0	0	0	0	0	0	0	1
$\{0\}$	0	0	1	0	1	1	0	1
$\{1\}$	0	1	0	0	0	0	0	1
$\{0,1\}$	0	1	1	1	1	0	0	1
$\{2\}$	1	0	0	0	0	0	0	1
$\{0,2\}$	1	0	1	1	1	0	1	1
$\{1,2\}$	1	1	0	1	1	0	0	1
$\{0,1,2\}$	1	1	1	1	0	0	0	1

We saw in Exercise 3.7 that

(a) $\mathrm{toffoli} = f_{\{0\}} \vee f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}}$;

(b) $\mathrm{maj} = f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}} \vee f_{\{0,1,2\}}$; equivalently,

$$\mathrm{maj}(x_0, x_1, x_2) = (x_0 \wedge x_1 \wedge \overline{x}_2) \vee (x_0 \wedge \overline{x}_1 \wedge x_2) \vee (\overline{x}_0 \wedge x_1 \wedge x_2) \vee (x_0 \wedge x_1 \wedge x_2).$$

Find the disjunctive normal form of $x_0 \implies x_1$.

Disjunctive Normal Form: Motivation

Recall that $f_J(x) = \bigwedge_{j \in J} x_j \wedge \bigwedge_{j \notin J} \overline{x}_j$. It is defined so that

$$f_J(x) = 1 \text{ if and only if } x_j = 1 \iff j \in J.$$

	x_2	x_1	x_0	$\mathrm{maj}(x_0, x_1, x_2)$	$\mathrm{toffoli}(x_0, x_1, x_2)$	$f_{\{0\}}$	$f_{\{0,2\}}$	True
$\varnothing$	0	0	0	0	0	0	0	1
$\{0\}$	0	0	1	0	1	1	0	1
$\{1\}$	0	1	0	0	0	0	0	1
$\{0,1\}$	0	1	1	1	1	0	0	1
$\{2\}$	1	0	0	0	0	0	0	1
$\{0,2\}$	1	0	1	1	1	0	1	1
$\{1,2\}$	1	1	0	1	1	0	0	1
$\{0,1,2\}$	1	1	1	1	0	0	0	1

We saw in Exercise 3.7 that

(a) $\mathrm{toffoli} = f_{\{0\}} \vee f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}}$;

(b) $\mathrm{maj} = f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}} \vee f_{\{0,1,2\}}$; equivalently,

$$\mathrm{maj}(x_0, x_1, x_2) = (x_0 \wedge x_1 \wedge \overline{x}_2) \vee (x_0 \wedge \overline{x}_1 \wedge x_2) \vee (\overline{x}_0 \wedge x_1 \wedge x_2) \vee (x_0 \wedge x_1 \wedge x_2).$$

Find the disjunctive normal form of $x_0 \implies x_1$. Answer. Since $x_0 \implies x_1$ is true if and only if

$$\{i : x_i = 1\} \in \big\{\varnothing, \{1\}, \{0,1\}\big\}$$

the disjunctive normal form is $(\overline{x_0} \wedge \overline{x_1}) \vee (\overline{x_0} \wedge x_1) \vee (x_0 \wedge x_1)$.

Disjunctive Normal Form: Motivation

Recall that $f_J(x) = \bigwedge_{j \in J} x_j \wedge \bigwedge_{j \notin J} \overline{x}_j$. It is defined so that

$$f_J(x) = 1 \text{ if and only if } x_j = 1 \iff j \in J.$$

	x_2	x_1	x_0	$\mathrm{maj}(x_0, x_1, x_2)$	$\mathrm{toffoli}(x_0, x_1, x_2)$	$f_{\{0\}}$	$f_{\{0,2\}}$	True
$\varnothing$	0	0	0	0	0	0	0	1
$\{0\}$	0	0	1	0	1	1	0	1
$\{1\}$	0	1	0	0	0	0	0	1
$\{0,1\}$	0	1	1	1	1	0	0	1
$\{2\}$	1	0	0	0	0	0	0	1
$\{0,2\}$	1	0	1	1	1	0	1	1
$\{1,2\}$	1	1	0	1	1	0	0	1
$\{0,1,2\}$	1	1	1	1	0	0	0	1

We saw in Exercise 3.7 that

(a) $\mathrm{toffoli} = f_{\{0\}} \vee f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}}$;

(b) $\mathrm{maj} = f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}} \vee f_{\{0,1,2\}}$; equivalently,

$$\mathrm{maj}(x_0, x_1, x_2) = (x_0 \wedge x_1 \wedge \overline{x}_2) \vee (x_0 \wedge \overline{x}_1 \wedge x_2) \vee (\overline{x}_0 \wedge x_1 \wedge x_2) \vee (x_0 \wedge x_1 \wedge x_2).$$

How many $\vee$ clauses (of the form $x_0 \wedge \overline{x}_1 \wedge x_2$) are in the disjunctive normal form of the always true function, shown in the rightmost column?

(A) 0 (B) 2 (C) 6 (D) 8

Disjunctive Normal Form: Motivation

Recall that $f_J(x) = \bigwedge_{j \in J} x_j \wedge \bigwedge_{j \notin J} \overline{x}_j$. It is defined so that

$$f_J(x) = 1 \text{ if and only if } x_j = 1 \iff j \in J.$$

	x_2	x_1	x_0	$\mathrm{maj}(x_0, x_1, x_2)$	$\mathrm{toffoli}(x_0, x_1, x_2)$	$f_{\{0\}}$	$f_{\{0,2\}}$	True
$\varnothing$	0	0	0	0	0	0	0	1
$\{0\}$	0	0	1	0	1	1	0	1
$\{1\}$	0	1	0	0	0	0	0	1
$\{0,1\}$	0	1	1	1	1	0	0	1
$\{2\}$	1	0	0	0	0	0	0	1
$\{0,2\}$	1	0	1	1	1	0	1	1
$\{1,2\}$	1	1	0	1	1	0	0	1
$\{0,1,2\}$	1	1	1	1	0	0	0	1

We saw in Exercise 3.7 that

(a) $\mathrm{toffoli} = f_{\{0\}} \vee f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}}$;

(b) $\mathrm{maj} = f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}} \vee f_{\{0,1,2\}}$; equivalently,

$$\mathrm{maj}(x_0, x_1, x_2) = (x_0 \wedge x_1 \wedge \overline{x}_2) \vee (x_0 \wedge \overline{x}_1 \wedge x_2) \vee (\overline{x}_0 \wedge x_1 \wedge x_2) \vee (x_0 \wedge x_1 \wedge x_2).$$

How many $\vee$ clauses (of the form $x_0 \wedge \overline{x}_1 \wedge x_2$) are in the disjunctive normal form of the always true function, shown in the rightmost column?

(A) 0 (B) 2 (C) 6 (D) 8

Disjunctive Normal Form: Motivation

Recall that $f_J(x) = \bigwedge_{j \in J} x_j \wedge \bigwedge_{j \notin J} \overline{x}_j$. It is defined so that

$$f_J(x) = 1 \text{ if and only if } x_j = 1 \iff j \in J.$$

	x_2	x_1	x_0	$\mathrm{maj}(x_0, x_1, x_2)$	$\mathrm{toffoli}(x_0, x_1, x_2)$	$f_{\{0\}}$	$f_{\{0,2\}}$	True
$\varnothing$	0	0	0	0	0	0	0	1
$\{0\}$	0	0	1	0	1	1	0	1
$\{1\}$	0	1	0	0	0	0	0	1
$\{0,1\}$	0	1	1	1	1	0	0	1
$\{2\}$	1	0	0	0	0	0	0	1
$\{0,2\}$	1	0	1	1	1	0	1	1
$\{1,2\}$	1	1	0	1	1	0	0	1
$\{0,1,2\}$	1	1	1	1	0	0	0	1

We saw in Exercise 3.7 that

(a) $\mathrm{toffoli} = f_{\{0\}} \vee f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}}$;

(b) $\mathrm{maj} = f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}} \vee f_{\{0,1,2\}}$; equivalently,

$$\mathrm{maj}(x_0, x_1, x_2) = (x_0 \wedge x_1 \wedge \overline{x}_2) \vee (x_0 \wedge \overline{x}_1 \wedge x_2) \vee (\overline{x}_0 \wedge x_1 \wedge x_2) \vee (x_0 \wedge x_1 \wedge x_2).$$

In fact the disjunctive normal form of the always true function is

$$(\overline{x}_0 \wedge \overline{x}_1 \wedge \overline{x}_2) \vee (x_0 \wedge \overline{x}_1 \wedge \overline{x}_2) \vee \cdots \vee (x_0 \wedge x_1 \wedge x_2).$$

Disjunctive Normal Form: Motivation

Recall that $f_J(x) = \bigwedge_{j \in J} x_j \wedge \bigwedge_{j \notin J} \overline{x}_j$. It is defined so that

$$f_J(x) = 1 \text{ if and only if } x_j = 1 \iff j \in J.$$

	x_2	x_1	x_0	$\mathrm{maj}(x_0, x_1, x_2)$	$\mathrm{toffoli}(x_0, x_1, x_2)$	$f_{\{0\}}$	$f_{\{0,2\}}$	True
$\varnothing$	0	0	0	0	0	0	0	1
$\{0\}$	0	0	1	0	1	1	0	1
$\{1\}$	0	1	0	0	0	0	0	1
$\{0,1\}$	0	1	1	1	1	0	0	1
$\{2\}$	1	0	0	0	0	0	0	1
$\{0,2\}$	1	0	1	1	1	0	1	1
$\{1,2\}$	1	1	0	1	1	0	0	1
$\{0,1,2\}$	1	1	1	1	0	0	0	1

We saw in Exercise 3.7 that

(a) $\mathrm{toffoli} = f_{\{0\}} \vee f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}}$;

(b) $\mathrm{maj} = f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}} \vee f_{\{0,1,2\}}$; equivalently,

$$\mathrm{maj}(x_0, x_1, x_2) = (x_0 \wedge x_1 \wedge \overline{x}_2) \vee (x_0 \wedge \overline{x}_1 \wedge x_2) \vee (\overline{x}_0 \wedge x_1 \wedge x_2) \vee (x_0 \wedge x_1 \wedge x_2).$$

What is the disjunctive normal form of the always false function?

Disjunctive Normal Form: Motivation

Recall that $f_J(x) = \bigwedge_{j \in J} x_j \wedge \bigwedge_{j \notin J} \overline{x}_j$. It is defined so that

$$f_J(x) = 1 \text{ if and only if } x_j = 1 \iff j \in J.$$

	x_2	x_1	x_0	$\mathrm{maj}(x_0, x_1, x_2)$	$\mathrm{toffoli}(x_0, x_1, x_2)$	$f_{\{0\}}$	$f_{\{0,2\}}$	True
$\varnothing$	0	0	0	0	0	0	0	1
$\{0\}$	0	0	1	0	1	1	0	1
$\{1\}$	0	1	0	0	0	0	0	1
$\{0,1\}$	0	1	1	1	1	0	0	1
$\{2\}$	1	0	0	0	0	0	0	1
$\{0,2\}$	1	0	1	1	1	0	1	1
$\{1,2\}$	1	1	0	1	1	0	0	1
$\{0,1,2\}$	1	1	1	1	0	0	0	1

We saw in Exercise 3.7 that

(a) $\mathrm{toffoli} = f_{\{0\}} \vee f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}}$;

(b) $\mathrm{maj} = f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}} \vee f_{\{0,1,2\}}$; equivalently,

$$\mathrm{maj}(x_0, x_1, x_2) = (x_0 \wedge x_1 \wedge \overline{x}_2) \vee (x_0 \wedge \overline{x}_1 \wedge x_2) \vee (\overline{x}_0 \wedge x_1 \wedge x_2) \vee (x_0 \wedge x_1 \wedge x_2).$$

What is the disjunctive normal form of the always false function?

Answer. The empty disjunction, i.e. the 'or' with no formulae. In symbols $\bigvee_{\emptyset} = 0$

Disjunctive Normal Form: Motivation

Recall that $f_J(x) = \bigwedge_{j \in J} x_j \wedge \bigwedge_{j \notin J} \overline{x}_j$. It is defined so that

$$f_J(x) = 1 \text{ if and only if } x_j = 1 \iff j \in J.$$

	x_2	x_1	x_0	$\mathrm{maj}(x_0, x_1, x_2)$	$\mathrm{toffoli}(x_0, x_1, x_2)$	$f_{\{0\}}$	$f_{\{0,2\}}$	True
$\varnothing$	0	0	0	0	0	0	0	1
$\{0\}$	0	0	1	0	1	1	0	1
$\{1\}$	0	1	0	0	0	0	0	1
$\{0,1\}$	0	1	1	1	1	0	0	1
$\{2\}$	1	0	0	0	0	0	0	1
$\{0,2\}$	1	0	1	1	1	0	1	1
$\{1,2\}$	1	1	0	1	1	0	0	1
$\{0,1,2\}$	1	1	1	1	0	0	0	1

We saw in Exercise 3.7 that

(a) $\mathrm{toffoli} = f_{\{0\}} \vee f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}}$;

(b) $\mathrm{maj} = f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}} \vee f_{\{0,1,2\}}$; equivalently,

$$\mathrm{maj}(x_0, x_1, x_2) = (x_0 \wedge x_1 \wedge \overline{x}_2) \vee (x_0 \wedge \overline{x}_1 \wedge x_2) \vee (\overline{x}_0 \wedge x_1 \wedge x_2) \vee (x_0 \wedge x_1 \wedge x_2).$$

What is the empty conjunction, i.e. the 'and' with no formulae. In symbols, what is $\bigwedge_{\emptyset}$?

Disjunctive Normal Form: Motivation

Recall that $f_J(x) = \bigwedge_{j \in J} x_j \wedge \bigwedge_{j \notin J} \overline{x}_j$. It is defined so that

$$f_J(x) = 1 \text{ if and only if } x_j = 1 \iff j \in J.$$

	x_2	x_1	x_0	$\mathrm{maj}(x_0, x_1, x_2)$	$\mathrm{toffoli}(x_0, x_1, x_2)$	$f_{\{0\}}$	$f_{\{0,2\}}$	True
$\varnothing$	0	0	0	0	0	0	0	1
$\{0\}$	0	0	1	0	1	1	0	1
$\{1\}$	0	1	0	0	0	0	0	1
$\{0,1\}$	0	1	1	1	1	0	0	1
$\{2\}$	1	0	0	0	0	0	0	1
$\{0,2\}$	1	0	1	1	1	0	1	1
$\{1,2\}$	1	1	0	1	1	0	0	1
$\{0,1,2\}$	1	1	1	1	0	0	0	1

We saw in Exercise 3.7 that

(a) $\mathrm{toffoli} = f_{\{0\}} \vee f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}}$;

(b) $\mathrm{maj} = f_{\{0,1\}} \vee f_{\{0,2\}} \vee f_{\{1,2\}} \vee f_{\{0,1,2\}}$; equivalently,

$$\mathrm{maj}(x_0, x_1, x_2) = (x_0 \wedge x_1 \wedge \overline{x}_2) \vee (x_0 \wedge \overline{x}_1 \wedge x_2) \vee (\overline{x}_0 \wedge x_1 \wedge x_2) \vee (x_0 \wedge x_1 \wedge x_2).$$

What is the empty conjunction, i.e. the 'and' with no formulae. In symbols, what is $\bigwedge_\emptyset$? Answer. The always true function: $\bigwedge_\emptyset = 1$.

Reminder of Seminars

- Mathematics Seminar 2pm Wednesday.
  - This week, Stacey Law (Cambridge).

    Sylow branching coefficients for symmetric groups

    Less technical that it sounds! Recommended.

  Look out for email with Zoom link.

- Information Security Group Seminar 11am Thursday.
  - This week Sikhar Patranabis (ETH Zurich)

    Minicrypt primitives with algebraic structure

  See `seminars.isg.rhul.ac.uk` for Zoom links.

Disjunctive Normal Form

Theorem 3.8 (Disjunctive Normal Form)

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a boolean function.

(i) *Suppose that the truth table of f has 1 in the rows labelled by the sets J for $J \in \mathcal{T}$. Then*

$$f = \bigvee_{J \in \mathcal{T}} f_J.$$

(ii) *If $\mathcal{T} \neq \mathcal{T}'$ then $\bigvee_{J\in\mathcal{T}} f_J \neq \bigvee_{J\in\mathcal{T}'} f_J$.*

This theorem says that every boolean function has a unique *disjunctive normal form* $\bigvee_{J\in\mathcal{T}} f_J$, for a suitable set $\mathcal{T}$.

Corollary 3.9

There are 2^{2^n} n-variable boolean functions.

Quiz: How many boolean functions are there of 4 variables?

(A) 16 (B) 256 (C) 1024 (D) 65536

Disjunctive Normal Form

Theorem 3.8 (Disjunctive Normal Form)

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a boolean function.

(i) *Suppose that the truth table of f has 1 in the rows labelled by the sets J for $J \in \mathcal{T}$. Then*

$$f = \bigvee_{J \in \mathcal{T}} f_J.$$

(ii) *If $\mathcal{T} \neq \mathcal{T}'$ then $\bigvee_{J\in\mathcal{T}} f_J \neq \bigvee_{J\in\mathcal{T}'} f_J$.*

This theorem says that every boolean function has a unique *disjunctive normal form* $\bigvee_{J\in\mathcal{T}} f_J$, for a suitable set $\mathcal{T}$.

Corollary 3.9

There are 2^{2^n} n-variable boolean functions.

Quiz: How many boolean functions are there of 4 variables?

(A) 16 (B) 256 (C) 1024 (D) 65536

Disjunctive Normal Form

Theorem 3.8 (Disjunctive Normal Form)

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a boolean function.

(i) *Suppose that the truth table of f has 1 in the rows labelled by the sets J for $J \in \mathcal{T}$. Then*

$$f = \bigvee_{J \in \mathcal{T}} f_J.$$

(ii) *If $\mathcal{T} \neq \mathcal{T}'$ then $\bigvee_{J\in\mathcal{T}} f_J \neq \bigvee_{J\in\mathcal{T}'} f_J$.*

This theorem says that every boolean function has a unique *disjunctive normal form* $\bigvee_{J\in\mathcal{T}} f_J$, for a suitable set $\mathcal{T}$.

Corollary 3.9

There are 2^{2^n} n-variable boolean functions.

Quiz: How many different possible columns are there for a truth table of a 3-variable boolean function? For instance, $0, 0, 0, 0, 1, 1, 1, 1$ is one possible column.

(A) 16 (B) 256 (C) 1024 (D) 65536

Disjunctive Normal Form

Theorem 3.8 (Disjunctive Normal Form)

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a boolean function.

(i) *Suppose that the truth table of f has 1 in the rows labelled by the sets J for $J \in \mathcal{T}$. Then*

$$f = \bigvee_{J \in \mathcal{T}} f_J.$$

(ii) *If $\mathcal{T} \neq \mathcal{T}'$ then $\bigvee_{J\in\mathcal{T}} f_J \neq \bigvee_{J\in\mathcal{T}'} f_J$.*

This theorem says that every boolean function has a unique *disjunctive normal form* $\bigvee_{J\in\mathcal{T}} f_J$, for a suitable set $\mathcal{T}$.

Corollary 3.9

There are 2^{2^n} n-variable boolean functions.

Quiz: How many different possible columns are there for a truth table of a 3-variable boolean function? For instance, $0, 0, 0, 0, 1, 1, 1, 1$ is one possible column.

(A) 16 (B) 256 (C) 1024 (D) 65536

All Boolean Functions of Two Variables: Exercise 3.10

By Corollary 3.9, there are 16 truth tables of 2-variable boolean functions. Using the true/false notation, the 8 for which $f(F, F) = F$ are shown below.

(a) What is a suitable label for the rightmost column?

(b) What is the disjunctive normal form of $x_0 + x_1$?

(A) $(x_0 \wedge \overline{x}_1) \vee (\overline{x}_0 \wedge x_1)$ (B) $(x_0 \wedge \overline{x}_1)$

(C) $(x_0 \wedge x_1) \vee (\overline{x}_0 \wedge \overline{x}_1)$ (D) $(x_0 \vee \overline{x}_1) \wedge (\overline{x}_0 \vee x_1))$

(c) Find the remaining disjunctive normal forms.

(d) What is a concise way to specify the remaining 8 functions?

	x_1	x_0	$x_0 \vee x_1$	x_0	x_1	$x_0 + x_1$	$x_0 \wedge x_1$	$x_0 \wedge \overline{x}_1$	$\overline{x}_0 \wedge x_1$	??
$\varnothing$	F	F	F	F	F	F	F	F	F	F
$\{0\}$	F	T	T	T	F	T	F	T	F	F
$\{1\}$	T	F	T	F	T	T	F	F	T	F
$\{0, 1\}$	T	T	T	T	T	F	T	F	F	F

All Boolean Functions of Two Variables: Exercise 3.10

By Corollary 3.9, there are 16 truth tables of 2-variable boolean functions. Using the true/false notation, the 8 for which $f(F, F) = F$ are shown below.

(a) What is a suitable label for the rightmost column?
Answer: F or 0, for the always false function. This is the empty disjunction: see quiz after Exercise 3.7.

(b) What is the disjunctive normal form of $x_0 + x_1$?
(A) $(x_0 \wedge \overline{x}_1) \vee (\overline{x}_0 \wedge x_1)$ (B) $(x_0 \wedge \overline{x}_1)$
(C) $(x_0 \wedge x_1) \vee (\overline{x}_0 \wedge \overline{x}_1)$ (D) $(x_0 \vee \overline{x}_1) \wedge (\overline{x}_0 \vee x_1))$

(c) Find the remaining disjunctive normal forms.

(d) What is a concise way to specify the remaining 8 functions?

	x_1	x_0	$x_0 \vee x_1$	x_0	x_1	$x_0 + x_1$	$x_0 \wedge x_1$	$x_0 \wedge \overline{x}_1$	$\overline{x}_0 \wedge x_1$	??
$\varnothing$	F	F	F	F	F	F	F	F	F	F
$\{0\}$	F	T	T	T	F	T	F	T	F	F
$\{1\}$	T	F	T	F	T	T	F	F	T	F
$\{0,1\}$	T	T	T	T	T	F	T	F	F	F

All Boolean Functions of Two Variables: Exercise 3.10

By Corollary 3.9, there are 16 truth tables of 2-variable boolean functions. Using the true/false notation, the 8 for which $f(F, F) = F$ are shown below.

(a) What is a suitable label for the rightmost column?
Answer: F or 0, for the always false function. This is the empty disjunction: see quiz after Exercise 3.7.

(b) What is the disjunctive normal form of $x_0 + x_1$?
(A) $(x_0 \wedge \overline{x}_1) \vee (\overline{x}_0 \wedge x_1)$ (B) $(x_0 \wedge \overline{x}_1)$
(C) $(x_0 \wedge x_1) \vee (\overline{x}_0 \wedge \overline{x}_1)$ (D) $(x_0 \vee \overline{x}_1) \wedge (\overline{x}_0 \vee x_1))$

(c) Find the remaining disjunctive normal forms.

(d) What is a concise way to specify the remaining 8 functions?

	x_1	x_0	$x_0 \vee x_1$	x_0	x_1	$x_0 + x_1$	$x_0 \wedge x_1$	$x_0 \wedge \overline{x}_1$	$\overline{x}_0 \wedge x_1$	??
$\varnothing$	F	F	F	F	F	F	F	F	F	F
$\{0\}$	F	T	T	T	F	T	F	T	F	F
$\{1\}$	T	F	T	F	T	T	F	F	T	F
$\{0,1\}$	T	T	T	T	T	F	T	F	F	F

All Boolean Functions of Two Variables: Exercise 3.10

By Corollary 3.9, there are 16 truth tables of 2-variable boolean functions. Using the true/false notation, the 8 for which $f(F, F) = F$ are shown below.

(a) What is a suitable label for the rightmost column?
Answer: F or 0, for the always false function. This is the empty disjunction: see quiz after Exercise 3.7.

(b) What is the disjunctive normal form of $x_0 + x_1$?
(A) $(x_0 \wedge \overline{x}_1) \vee (\overline{x}_0 \wedge x_1)$ (B) $(x_0 \wedge \overline{x}_1)$
(C) $(x_0 \wedge x_1) \vee (\overline{x}_0 \wedge \overline{x}_1)$ (D) $(x_0 \vee \overline{x}_1) \wedge (\overline{x}_0 \vee x_1))$

(c) Find the remaining disjunctive normal forms.
Example: the DNF of x_0 is $(x_0 \wedge x_1) \vee (x_0 \wedge \overline{x}_1)$.

(d) What is a concise way to specify the remaining 8 functions?

	x_1	x_0	$x_0 \vee x_1$	x_0	x_1	$x_0 + x_1$	$x_0 \wedge x_1$	$x_0 \wedge \overline{x}_1$	$\overline{x}_0 \wedge x_1$	??
$\varnothing$	F	F	F	F	F	F	F	F	F	F
$\{0\}$	F	T	T	T	F	T	F	T	F	F
$\{1\}$	T	F	T	F	T	T	F	F	T	F
$\{0,1\}$	T	T	T	T	T	F	T	F	F	F

All Boolean Functions of Two Variables: Exercise 3.10

By Corollary 3.9, there are 16 truth tables of 2-variable boolean functions. Using the true/false notation, the 8 for which $f(F, F) = F$ are shown below.

(a) What is a suitable label for the rightmost column?
Answer: F or 0, for the always false function. This is the empty disjunction: see quiz after Exercise 3.7.

(b) What is the disjunctive normal form of $x_0 + x_1$?
(A) $(x_0 \wedge \overline{x}_1) \vee (\overline{x}_0 \wedge x_1)$ (B) $(x_0 \wedge \overline{x}_1)$
(C) $(x_0 \wedge x_1) \vee (\overline{x}_0 \wedge \overline{x}_1)$ (D) $(x_0 \vee \overline{x}_1) \wedge (\overline{x}_0 \vee x_1))$

(c) Find the remaining disjunctive normal forms.
Example: the DNF of x_0 is $(x_0 \wedge x_1) \vee (x_0 \wedge \overline{x}_1)$.

(d) What is a concise way to specify the remaining 8 functions?
Answer: $\overline{x_0 \vee x_1}, \overline{x_0}, \overline{x}_1, \overline{x_0 + x_1}, \ldots$ i.e. just negate!

	x_1	x_0	$x_0 \vee x_1$	x_0	x_1	$x_0 + x_1$	$x_0 \wedge x_1$	$x_0 \wedge \overline{x}_1$	$\overline{x}_0 \wedge x_1$	??
$\varnothing$	F	F	F	F	F	F	F	F	F	F
$\{0\}$	F	T	T	T	F	T	F	T	F	F
$\{1\}$	T	F	T	F	T	T	F	F	T	F
$\{0,1\}$	T	T	T	T	T	F	T	F	F	F

Algebraic Normal Form

In $\mathbb{F}_2$ we have $0^2 = 0$ and $1^2 = 1$. Therefore the boolean functions $f(x_1) = x_1^2$ and $f(x_1) = x_1$ are equal. Hence, as seen in Exercise 3.2, multivariable polynomials over $\mathbb{F}_2$ do not need squares or higher powers of the variables. Similarly, since $2x_1 = 0$, the only coefficients needed are the bits 0 and 1. For instance,

$$x_0 + x_0x_2^2x_3^3 + x_0^2 + x_2x_3$$

is the same boolean function as $x_2x_3 + x_0x_2x_3$.

Given $I \subseteq \{0, 1, \ldots, n-1\}$, let

$$x_I = \prod_{i \in I} x_i.$$

We say the x_I are *boolean monomials*. By definition (or convention if you prefer), $x_\varnothing = 1$. For example, $x_{\{1,2\}} = x_1x_2$. It is one of the three boolean monomial summands of

$$\mathrm{maj}(x_0, x_1, x_2) = x_0x_1 + x_1x_2 + x_2x_0 = x_{\{0,1\}} + x_{\{1,2\}} + x_{\{0,2\}}.$$

Motivation for Algebraic Normal Form

The functions f_J so useful for proving Theorem 3.8 have a particularly simple form as polynomials:

$$f_J(x) = \prod_{j \in J} x_j \prod_{j \notin J} \overline{x}_j.$$

Exercise 3.11

(i) Define the 3-variable boolean function

$$g(x_0, x_1, x_2) = \begin{cases} 1 & \text{if } x_0 = x_1 = x_2 = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Express g as sum of boolean monomials. How many monomials do you need?

(A) 1 (B) 4 (C) 7 (D) 8

(ii) What is the negation $\overline{g}$ as a sum of boolean monomials?

Motivation for Algebraic Normal Form

The functions f_J so useful for proving Theorem 3.8 have a particularly simple form as polynomials:

$$f_J(x) = \prod_{j \in J} x_j \prod_{j \notin J} \overline{x}_j.$$

Exercise 3.11

(i) Define the 3-variable boolean function

$$g(x_0, x_1, x_2) = \begin{cases} 1 & \text{if } x_0 = x_1 = x_2 = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Express g as sum of boolean monomials. How many monomials do you need?

(A) 1 (B) 4 (C) 7 (D) 8

Since

$$\begin{aligned} \overline{x}_0\overline{x}_1\overline{x}_2 &= (1 + x_0)(1 + x_1)(1 + x_2) \\ &= 1 + x_0 + x_1 + x_2 + x_0x_1 + x_0x_2 + x_1x_2 + x_0x_1x_2 \end{aligned}$$

(ii) What is the negation $\overline{g}$ as a sum of boolean monomials?

Motivation for Algebraic Normal Form

The functions f_J so useful for proving Theorem 3.8 have a particularly simple form as polynomials:

$$f_J(x) = \prod_{j \in J} x_j \prod_{j \notin J} \overline{x}_j.$$

Exercise 3.11

(i) Define the 3-variable boolean function

$$g(x_0, x_1, x_2) = \begin{cases} 1 & \text{if } x_0 = x_1 = x_2 = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Express g as sum of boolean monomials. How many monomials do you need?

(A) 1 (B) 4 (C) 7 (D) 8

Since

$$\begin{aligned} \overline{x}_0\overline{x}_1\overline{x}_2 &= (1 + x_0)(1 + x_1)(1 + x_2) \\ &= 1 + x_0 + x_1 + x_2 + x_0x_1 + x_0x_2 + x_1x_2 + x_0x_1x_2 \end{aligned}$$

(ii) What is the negation $\overline{g}$ as a sum of boolean monomials?

Answer. You can negate *anything* by adding 1 to it, so just get rid of the 1 in the expression for g.

Motivation for Algebraic Normal Form

The functions f_J so useful for proving Theorem 3.8 have a particularly simple form as polynomials:

$$f_J(x) = \prod_{j \in J} x_j \prod_{j \notin J} \overline{x}_j.$$

Exercise 3.11

(i) Define the 3-variable boolean function

$$g(x_0, x_1, x_2) = \begin{cases} 1 & \text{if } x_0 = x_1 = x_2 = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Express g as sum of boolean monomials. How many monomials do you need?

(A) 1 (B) 4 (C) 7 (D) 8

Since

$$\begin{aligned} \overline{x}_0\overline{x}_1\overline{x}_2 &= (1 + x_0)(1 + x_1)(1 + x_2) \\ &= 1 + x_0 + x_1 + x_2 + x_0x_1 + x_0x_2 + x_1x_2 + x_0x_1x_2 \end{aligned}$$

(iii) True or false: if a 3-variable has $x_0x_1x_2$ as a monomial, then it is 1 when $x_0 = x_1 = x_2 = 1$.

(A) False (B) True

Motivation for Algebraic Normal Form

The functions f_J so useful for proving Theorem 3.8 have a particularly simple form as polynomials:

$$f_J(x) = \prod_{j \in J} x_j \prod_{j \notin J} \overline{x}_j.$$

Exercise 3.11

(i) Define the 3-variable boolean function

$$g(x_0, x_1, x_2) = \begin{cases} 1 & \text{if } x_0 = x_1 = x_2 = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Express g as sum of boolean monomials. How many monomials do you need?

(A) 1 (B) 4 (C) 7 (D) 8

Since

$$\begin{aligned} \overline{x}_0\overline{x}_1\overline{x}_2 &= (1 + x_0)(1 + x_1)(1 + x_2) \\ &= 1 + x_0 + x_1 + x_2 + x_0x_1 + x_0x_2 + x_1x_2 + x_0x_1x_2 \end{aligned}$$

(iii) True or false: if a 3-variable has $x_0x_1x_2$ as a monomial, then it is 1 when $x_0 = x_1 = x_2 = 1$.

(A) False (B) True

Motivation for Algebraic Normal Form

The functions f_J so useful for proving Theorem 3.8 have a particularly simple form as polynomials:

$$f_J(x) = \prod_{j \in J} x_j \prod_{j \notin J} \overline{x}_j.$$

Exercise 3.11

(i) Define the 3-variable boolean function

$$g(x_0, x_1, x_2) = \begin{cases} 1 & \text{if } x_0 = x_1 = x_2 = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Express g as sum of boolean monomials. How many monomials do you need?

(A) 1 (B) 4 (C) 7 (D) 8

Since

$$\begin{aligned} \overline{x}_0\overline{x}_1\overline{x}_2 &= (1 + x_0)(1 + x_1)(1 + x_2) \\ &= 1 + x_0 + x_1 + x_2 + x_0x_1 + x_0x_2 + x_1x_2 + x_0x_1x_2 \end{aligned}$$

(iii) True or false: if a 3-variable has $x_0x_1x_2$ as a monomial, then it is 1 when $x_0 = x_1 = x_2 = 1$. Example: $x_0 + x_1 + x_2 + x_0x_1x_2$ is zero when $x_0 = x_1 = x_2 = 1$. See coefficient formula later.

Toffoli function in Algebraic Normal Form

We saw that the disjunctive normal form, written using the f_J functions, of the Toffoli function is

$$\mathrm{toffoli}(x_0, x_1, x_2) = f_{\{0\}} + f_{\{0,1\}} + f_{\{0,2\}} + f_{\{1,2\}}.$$

Hence or otherwise write it as a sum of boolean monomials.

Toffoli function in Algebraic Normal Form

We saw that the disjunctive normal form, written using the f_J functions, of the Toffoli function is

$$\mathrm{toffoli}(x_0, x_1, x_2) = f_{\{0\}} + f_{\{0,1\}} + f_{\{0,2\}} + f_{\{1,2\}}.$$

Hence or otherwise write it as a sum of boolean monomials.

- The mechanical way to do this is

$$\begin{aligned}
\mathrm{toffoli} &= f_{\{0\}} + f_{\{0,1\}} + f_{\{0,2\}} + f_{\{1,2\}} \\
&= x_0(1+x_1)(1+x_2) + x_0x_1(1+x_2) + x_0(1+x_1)x_2 + (1+x_0)x_1x_2 \\
&= \big(x_0 + x_0x_1 + x_0x_2 + x_0x_1x_2\big) + \big(x_0x_1 + x_0x_1x_2\big) \\
&\qquad + \big(x_0x_2 + x_0x_1x_2\big) + \big(x_1x_2 + x_0x_1x_2\big) \\
&= x_0 + x_1x_2
\end{aligned}$$

Toffoli function in Algebraic Normal Form

We saw that the disjunctive normal form, written using the f_J functions, of the Toffoli function is

$$\mathrm{toffoli}(x_0, x_1, x_2) = f_{\{0\}} + f_{\{0,1\}} + f_{\{0,2\}} + f_{\{1,2\}}.$$

Hence or otherwise write it as a sum of boolean monomials.

- The mechanical way to do this is

$$\begin{aligned}\mathrm{toffoli} &= f_{\{0\}} + f_{\{0,1\}} + f_{\{0,2\}} + f_{\{1,2\}} \\ &= x_0(1+x_1)(1+x_2) + x_0x_1(1+x_2) + x_0(1+x_1)x_2 + (1+x_0)x_1x_2 \\ &= \big(x_0 + x_0x_1 + x_0x_2 + x_0x_1x_2\big) + \big(x_0x_1 + x_0x_1x_2\big) \\ &\qquad + \big(x_0x_2 + x_0x_1x_2\big) + \big(x_1x_2 + x_0x_1x_2\big) \\ &= x_0 + x_1x_2\end{aligned}$$

- Better: go back to Example 3.6 and use that $\mathrm{toffoli}(x_0, x_1, x_2)$ is 1 if and only if $x_1x_2 = 0$ and $x_0 = 1$, or $x_1x_2 = 1$ and $x_0 = 0$, and so

$$\mathrm{toffoli}(x_0, x_1, x_2) = \overline{x_1x_2}x_0 + x_1x_2\overline{x_0} = (1+x_1x_2)x_0 + x_1x_2(1+x_0)$$

which expands to $x_0 + x_1x_2$.

Algebraic Normal Form

It is only a small generalization of the Toffoli example just seen to prove the existence part of the following theorem. There is a very neat way to prove uniqueness, using the result from Corollary 3.9 that there are exactly 2^{2^n} boolean functions of n variables.

Theorem 3.12

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be an n-variable boolean function.

(a) *There exist coefficients $b_J \in \{0, 1\}$, one for each $J \subseteq \{0, 1, \ldots, n-1\}$ such that*

$$f = \sum_{J \subseteq \{0,1,\ldots,n\}} b_J f_J.$$

(b) *There exist unique coefficients $c_I \in \{0, 1\}$, one for each $I \subseteq \{0, 1, \ldots, n-1\}$, such that*

$$f = \sum_{I \subseteq \{0,1,\ldots,n-1\}} c_I x_I.$$

Algebraic Normal Form

It is only a small generalization of the Toffoli example just seen to prove the existence part of the following theorem. There is a very neat way to prove uniqueness, using the result from Corollary 3.9 that there are exactly 2^{2^n} boolean functions of n variables.

Theorem 3.12

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be an n-variable boolean function.

(a) *There exist coefficients $b_J \in \{0, 1\}$, one for each $J \subseteq \{0, 1, \ldots, n-1\}$ such that*

$$f = \sum_{J \subseteq \{0,1,\ldots,n\}} b_J f_J.$$

(b) *There exist unique coefficients $c_I \in \{0, 1\}$, one for each $I \subseteq \{0, 1, \ldots, n-1\}$, such that*

$$f = \sum_{I \subseteq \{0,1,\ldots,n-1\}} c_I x_I.$$

The expression for f in (b) is called the *algebraic normal form* of f.

Exercise: deduce from the uniqueness of disjunctive normal form that the coefficients b_J in (a) are also unique.

Motivation for Coefficient Formula

Exercise 3.13

Let $f(x, y, z) = 1 + x + xz + yz + xyz$ and let

$$g(x, y, z) = f(0, y, z) + f(1, y, z).$$

(i) What information does $f(0, 0, 0)$ tell us about f?

(ii) Find the algebraic normal form of g. What is the connection with the algebraic normal form of f?

(iii) What does $g(0, 0, 0) = f(0, 0, 0) + f(1, 0, 0)$ tells us about g? What does it tell us about f?

Motivation for Coefficient Formula

Exercise 3.13

Let $f(x, y, z) = 1 + x + xz + yz + xyz$ and let

$$g(x, y, z) = f(0, y, z) + f(1, y, z).$$

(i) What information does $f(0, 0, 0)$ tell us about f?

(ii) Find the algebraic normal form of g. What is the connection with the algebraic normal form of f?

(iii) What does $g(0, 0, 0) = f(0, 0, 0) + f(1, 0, 0)$ tells us about g? What does it tell us about f?

Answers.

(i) $f(0, 0, 0)$ is the constant term in f, namely 1.

Motivation for Coefficient Formula

Exercise 3.13

Let $f(x, y, z) = 1 + x + xz + yz + xyz$ and let

$$g(x, y, z) = f(0, y, z) + f(1, y, z).$$

(i) What information does $f(0, 0, 0)$ tell us about f?

(ii) Find the algebraic normal form of g. What is the connection with the algebraic normal form of f?

(iii) What does $g(0, 0, 0) = f(0, 0, 0) + f(1, 0, 0)$ tells us about g? What does it tell us about f?

Answers.

(i) $f(0, 0, 0)$ is the constant term in f, namely 1.

(ii) $g(x, y, z) = 1 + z + yz$ in algebraic normal form. You can get this from the algebraic normal form of f by differentiating in the usual way! That is, delete any monomial not having x, and cancel x from those that do have it.

Motivation for Coefficient Formula

Exercise 3.13

Let $f(x, y, z) = 1 + x + xz + yz + xyz$ and let

$$g(x, y, z) = f(0, y, z) + f(1, y, z).$$

(i) What information does $f(0, 0, 0)$ tell us about f?

(ii) Find the algebraic normal form of g. What is the connection with the algebraic normal form of f?

(iii) What does $g(0, 0, 0) = f(0, 0, 0) + f(1, 0, 0)$ tells us about g? What does it tell us about f?

Answers.

(i) $f(0, 0, 0)$ is the constant term in f, namely 1.

(ii) $g(x, y, z) = 1 + z + yz$ in algebraic normal form. You can get this from the algebraic normal form of f by differentiating in the usual way! That is, delete any monomial not having x, and cancel x from those that do have it.

(iii) $g(0, 0, 0) = 1$ is the constant term of g, which corresponds to the x in f. Hence the algebraic normal form of f has x.

Motivation for Coefficient Formula

Exercise 3.13

Let $f(x, y, z) = 1 + x + xz + yz + xyz$ and let

$$g(x, y, z) = f(0, y, z) + f(1, y, z).$$

(i) What information does $f(0, 0, 0)$ tell us about f?

(ii) Find the algebraic normal form of g. What is the connection with the algebraic normal form of f?

(iii) What does $g(0, 0, 0) = f(0, 0, 0) + f(1, 0, 0)$ tells us about g? What does it tell us about f?

Given $i \in \{0, 1, \ldots, n-1\}$, define $\Delta^{(i)} = (0, \ldots, 1, \ldots, 0)$, where the 1 is in position i. The *discrete derivative in position i* of an n-variable boolean function f is the boolean function, $(D_i f)$ defined by

$$(D_i f)(x) = f(x + \Delta^{(i)}) + f(x).$$

Since x and $x + \Delta^{(i)}$ are, in some order, $(x_0, \ldots, 0, \ldots, x_{n-1}) \in \mathbb{F}_2^n$ and $(x_0, \ldots, 1, \ldots, x_{n-1}) \in \mathbb{F}_2^n$, an equivalent definition is $(D_i f)(x_0, \ldots, x_i, \ldots, x_{n-1}) = f(x_0, \ldots, 1, \ldots, x_n) + f(x_0, \ldots, 0, \ldots, x_n)$.

Coefficients Via the Discrete Derivative

Recall that

$$(D_i f)(x_0, \ldots, x_{n-1}) = f(x_0, \ldots, 1, \ldots, x_n) + f(x_0, \ldots, 0, \ldots, x_n).$$

where the 0 and 1 are in position i.

- $D_i f$ does not depend on x_i

(A) False (B) True

Restated using the discrete derivative, in Exercise 3.13 we had

$$f(x_0, x_1, x_2) = 1 + x_0 + x_0x_2 + x_1x_2 + x_0x_1x_2$$

and considered $g = D_0 f$ and, in plenary session, $h = D_2 g = D_2 D_0 f$.

$$(D_0 f)(x_0, x_1, x_2) = 0 + 1 + x_0 + 0 + x_1x_2 = 1 + x_0 + x_1x_2$$
$$(D_2 g)(x_0, x_1, x_2) = 0 + 0 + x_1 = x_1.$$

So $(D_0 f)(0,0,0) = (D_2 D_0 f)(0,0,0) = 1$ giving the coefficients of x_0 and x_0x_2 in f. Written out as a sum

$$\begin{aligned}(D_2 D_0 f)(0,0,0) &= g(0,0,0) + g(0,0,1) \\ &= f(0,0,0) + f(1,0,0) + f(0,0,1) + f(1,0,1) = 1.\end{aligned}$$

Coefficients Via the Discrete Derivative

Recall that

$$(D_i f)(x_0, \ldots, x_{n-1}) = f(x_0, \ldots, 1, \ldots, x_n) + f(x_0, \ldots, 0, \ldots, x_n).$$

where the 0 and 1 are in position i.

- $D_i f$ does not depend on x_i

(A) False (B) True

Since x_i does not appear on the right-hand side.

Restated using the discrete derivative, in Exercise 3.13 we had

$$f(x_0, x_1, x_2) = 1 + x_0 + x_0x_2 + x_1x_2 + x_0x_1x_2$$

and considered $g = D_0 f$ and, in plenary session, $h = D_2 g = D_2 D_0 f$.

$$(D_0 f)(x_0, x_1, x_2) = 0 + 1 + x_0 + 0 + x_1x_2 = 1 + x_0 + x_1x_2$$
$$(D_2 g)(x_0, x_1, x_2) = 0 + 0 + x_1 = x_1.$$

So $(D_0 f)(0,0,0) = (D_2 D_0 f)(0,0,0) = 1$ giving the coefficients of x_0 and x_0x_2 in f. Written out as a sum

$$\begin{aligned}(D_2 D_0 f)(0,0,0) &= g(0,0,0) + g(0,0,1) \\ &= f(0,0,0) + f(1,0,0) + f(0,0,1) + f(1,0,1) = 1.\end{aligned}$$

Quiz on Discrete Derivative (1)

The function $f_{\{2\}}$ which is true if and only if x_0, x_1 are 0 and x_2 is 1 has product form $(1 + x_0)(1 + x_1)x_2$.

- What is $D_2 f_{\{2\}}$?
  (A) $1 + x_0$ (B) $1 + x_0 + x_1 + x_0x_2$ (C) $(1 + x_0)(1 + x_1)$ (D) $(1 + x_0)x_1$
- What is $D_0 D_1 f_{\{2\}}$?
  (A) x_0 (B) x_2 (C) $x_0 + x_2$ (D) $1 + x_2$
- What is $D_0 D_1 D_2 f_{\{2\}}$?
  (A) 0 (B) 1 (C) x_0 (D) $1 + x_0$
- What is $D_2(f_{\{2\}} + x_1x_2)$? [*Hint:* derivatives are linear.]
  (A) $1 + x_0 + x_1$ (B) $1 + x_1 + x_0x_2$ (C) $(1 + x_0)(1 + x_1) + x_1$ (D) x_0x_1
- True or false: $(D_2 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True
- True or false: $(D_0 D_1 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True
- True or false: $(D_0 D_1 D_2 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True

Quiz on Discrete Derivative (1)

The function $f_{\{2\}}$ which is true if and only if x_0, x_1 are 0 and x_2 is 1 has product form $(1 + x_0)(1 + x_1)x_2$.

- What is $D_2 f_{\{2\}}$?
  (A) $1 + x_0$ (B) $1 + x_0 + x_1 + x_0x_2$ (C) $(1 + x_0)(1 + x_1)$ (D) $(1 + x_0)x_1$
- What is $D_0 D_1 f_{\{2\}}$?
  (A) x_0 (B) x_2 (C) $x_0 + x_2$ (D) $1 + x_2$
- What is $D_0 D_1 D_2 f_{\{2\}}$?
  (A) 0 (B) 1 (C) x_0 (D) $1 + x_0$
- What is $D_2(f_{\{2\}} + x_1x_2)$? [*Hint:* derivatives are linear.]
  (A) $1 + x_0 + x_1$ (B) $1 + x_1 + x_0x_2$ (C) $(1 + x_0)(1 + x_1) + x_1$ (D) x_0x_1
- True or false: $(D_2 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True
- True or false: $(D_0 D_1 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True
- True or false: $(D_0 D_1 D_2 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True

Quiz on Discrete Derivative (1)

The function $f_{\{2\}}$ which is true if and only if x_0, x_1 are 0 and x_2 is 1 has product form $(1 + x_0)(1 + x_1)x_2$.

- What is $D_2 f_{\{2\}}$?
  (A) $1 + x_0$ (B) $1 + x_0 + x_1 + x_0x_2$ (C) $(1 + x_0)(1 + x_1)$ (D) $(1 + x_0)x_1$
- What is $D_0 D_1 f_{\{2\}}$?
  (A) x_0 (B) x_2 (C) $x_0 + x_2$ (D) $1 + x_2$
- What is $D_0 D_1 D_2 f_{\{2\}}$?
  (A) 0 (B) 1 (C) x_0 (D) $1 + x_0$
- What is $D_2(f_{\{2\}} + x_1x_2)$? [*Hint:* derivatives are linear.]
  (A) $1 + x_0 + x_1$ (B) $1 + x_1 + x_0x_2$ (C) $(1 + x_0)(1 + x_1) + x_1$ (D) x_0x_1
- True or false: $(D_2 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True
- True or false: $(D_0 D_1 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True
- True or false: $(D_0 D_1 D_2 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True

Quiz on Discrete Derivative (1)

The function $f_{\{2\}}$ which is true if and only if x_0, x_1 are 0 and x_2 is 1 has product form $(1 + x_0)(1 + x_1)x_2$.

- What is $D_2 f_{\{2\}}$?
  (A) $1 + x_0$ (B) $1 + x_0 + x_1 + x_0x_2$ (C) $(1 + x_0)(1 + x_1)$ (D) $(1 + x_0)x_1$
- What is $D_0 D_1 f_{\{2\}}$?
  (A) x_0 (B) x_2 (C) $x_0 + x_2$ (D) $1 + x_2$
- What is $D_0 D_1 D_2 f_{\{2\}}$?
  (A) 0 (B) 1 (C) x_0 (D) $1 + x_0$
- What is $D_2(f_{\{2\}} + x_1x_2)$? [*Hint:* derivatives are linear.]
  (A) $1 + x_0 + x_1$ (B) $1 + x_1 + x_0x_2$ (C) $(1 + x_0)(1 + x_1) + x_1$ (D) x_0x_1
- True or false: $(D_2 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True
- True or false: $(D_0 D_1 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True
- True or false: $(D_0 D_1 D_2 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True

Quiz on Discrete Derivative (1)

The function $f_{\{2\}}$ which is true if and only if x_0, x_1 are 0 and x_2 is 1 has product form $(1 + x_0)(1 + x_1)x_2$.

- What is $D_2 f_{\{2\}}$?
  (A) $1 + x_0$ (B) $1 + x_0 + x_1 + x_0x_2$ (C) $(1 + x_0)(1 + x_1)$ (D) $(1 + x_0)x_1$
- What is $D_0 D_1 f_{\{2\}}$?
  (A) x_0 (B) x_2 (C) $x_0 + x_2$ (D) $1 + x_2$
- What is $D_0 D_1 D_2 f_{\{2\}}$?
  (A) 0 (B) 1 (C) x_0 (D) $1 + x_0$
- What is $D_2(f_{\{2\}} + x_1x_2)$? [*Hint:* derivatives are linear.]
  (A) $1 + x_0 + x_1$ (B) $1 + x_1 + x_0x_2$ (C) $(1 + x_0)(1 + x_1) + x_1$ (D) x_0x_1
- True or false: $(D_2 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True
- True or false: $(D_0 D_1 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True
- True or false: $(D_0 D_1 D_2 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True

Quiz on Discrete Derivative (1)

The function $f_{\{2\}}$ which is true if and only if x_0, x_1 are 0 and x_2 is 1 has product form $(1 + x_0)(1 + x_1)x_2$.

- What is $D_2 f_{\{2\}}$?
  (A) $1 + x_0$ (B) $1 + x_0 + x_1 + x_0x_2$ (C) $(1 + x_0)(1 + x_1)$ (D) $(1 + x_0)x_1$
- What is $D_0 D_1 f_{\{2\}}$?
  (A) x_0 (B) x_2 (C) $x_0 + x_2$ (D) $1 + x_2$
- What is $D_0 D_1 D_2 f_{\{2\}}$?
  (A) 0 (B) 1 (C) x_0 (D) $1 + x_0$
- What is $D_2(f_{\{2\}} + x_1x_2)$? [*Hint:* derivatives are linear.]
  (A) $1 + x_0 + x_1$ (B) $1 + x_1 + x_0x_2$ (C) $(1 + x_0)(1 + x_1) + x_1$ (D) x_0x_1
- True or false: $(D_2 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True
- True or false: $(D_0 D_1 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True
- True or false: $(D_0 D_1 D_2 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True

Quiz on Discrete Derivative (1)

The function $f_{\{2\}}$ which is true if and only if x_0, x_1 are 0 and x_2 is 1 has product form $(1 + x_0)(1 + x_1)x_2$.

- What is $D_2 f_{\{2\}}$?
  (A) $1 + x_0$ (B) $1 + x_0 + x_1 + x_0x_2$ (C) $(1 + x_0)(1 + x_1)$ (D) $(1 + x_0)x_1$
- What is $D_0 D_1 f_{\{2\}}$?
  (A) x_0 (B) x_2 (C) $x_0 + x_2$ (D) $1 + x_2$
- What is $D_0 D_1 D_2 f_{\{2\}}$?
  (A) 0 (B) 1 (C) x_0 (D) $1 + x_0$
- What is $D_2(f_{\{2\}} + x_1x_2)$? [*Hint:* derivatives are linear.]
  (A) $1 + x_0 + x_1$ (B) $1 + x_1 + x_0x_2$ (C) $(1 + x_0)(1 + x_1) + x_1$ (D) x_0x_1
- True or false: $(D_2 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True
- True or false: $(D_0 D_1 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True
- True or false: $(D_0 D_1 D_2 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True

Quiz on Discrete Derivative (1)

The function $f_{\{2\}}$ which is true if and only if x_0, x_1 are 0 and x_2 is 1 has product form $(1 + x_0)(1 + x_1)x_2$.

- What is $D_2 f_{\{2\}}$?
  (A) $1 + x_0$ (B) $1 + x_0 + x_1 + x_0x_2$ (C) $(1 + x_0)(1 + x_1)$ (D) $(1 + x_0)x_1$
- What is $D_0D_1 f_{\{2\}}$?
  (A) x_0 (B) x_2 (C) $x_0 + x_2$ (D) $1 + x_2$
- What is $D_0D_1D_2 f_{\{2\}}$?
  (A) 0 (B) 1 (C) x_0 (D) $1 + x_0$
- What is $D_2(f_{\{2\}} + x_1x_2)$? [*Hint:* derivatives are linear.]
  (A) $1 + x_0 + x_1$ (B) $1 + x_1 + x_0x_2$ (C) $(1 + x_0)(1 + x_1) + x_1$ (D) x_0x_1
- True or false: $(D_2 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True
- True or false: $(D_0D_1 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True
- True or false: $(D_0D_1D_2 f_{\{2\}})(0, 0, 0) = 1$?
  (A) False (B) True

Correspond to the final three questions, the algebraic normal form of $f_{\{2\}}$, given by multiplying out $(1 + x_0)(1 + x_1)x_2$ has the monomials x_2 and $x_0x_1x_2$ but does not have x_0x_1.

Quiz on Discrete Derivative (2)

For $i \in \{0, 1, \ldots, n-1\}$, let $\Delta^{(i)} = (0, \ldots, 1, \ldots, 0) \in \mathbb{F}_2^n$, where the 1 is in position i. Thus if f is an n-variable boolean function,

$$(D_i f)(x) = f(x + \Delta^{(i)}) + f(x)$$

for all $x \in \mathbb{F}_2^n$.

- True or false: $D_i D_j f = D_j D_i f$ for all $i, j \in \{0, 1, \ldots, n-1\}$? [*Hint:* write each side evaluated at $x \in \mathbb{F}_2^n$ using $\Delta^{(i)}$ and $\Delta^{(j)}$.]

(A) False (B) True

Quiz on Discrete Derivative (2)

For $i \in \{0, 1, \ldots, n-1\}$, let $\Delta^{(i)} = (0, \ldots, 1, \ldots, 0) \in \mathbb{F}_2^n$, where the 1 is in position i. Thus if f is an n-variable boolean function,

$$(D_i f)(x) = f(x + \Delta^{(i)}) + f(x)$$

for all $x \in \mathbb{F}_2^n$.

- True or false: $D_i D_j f = D_j D_i f$ for all $i, j \in \{0, 1, \ldots, n-1\}$? [*Hint:* write each side evaluated at $x \in \mathbb{F}_2^n$ using $\Delta^{(i)}$ and $\Delta^{(j)}$.]

(A) False (B) True

$$\begin{aligned}
(D_i D_j f)(x) &= D_i\big(f(x + \Delta^{(j)}) + f(x)\big) \\
&= \big(f(x + \Delta^{(j)} + \Delta^{(i)}) + f(x + \Delta^{(i)})\big) + \big(f(x + \Delta^{(j)} + f(x)\big) \\
&= \big(f(x + \Delta^{(i)} + \Delta^{(j)}) + f(x + \Delta^{(j)})\big) + \big(f(x + \Delta^{(i)} + f(x)\big) \\
&= D_j\big(f(x + \Delta^{(i)}) + f(x)\big)
\end{aligned}$$

This should remind you of the usual rule that partial derivatives such as $\frac{\partial}{\partial x}$ and $\frac{\partial}{\partial y}$ commute. (For real functions this needs some technical assumptions — it's *always* true for the discrete derivative.)

Quiz on Discrete Derivative (2)

For $i \in \{0, 1, \ldots, n-1\}$, let $\Delta^{(i)} = (0, \ldots, 1, \ldots, 0) \in \mathbb{F}_2^n$, where the 1 is in position i. Thus if f is an n-variable boolean function,

$$(D_i f)(x) = f(x + \Delta^{(i)}) + f(x)$$

for all $x \in \mathbb{F}_2^n$.

- What is $D_i D_i f$, for any function f?

  (A) 0 (B) 1 (C) $D_i f$ (D) depends on f

Quiz on Discrete Derivative (2)

For $i \in \{0, 1, \ldots, n-1\}$, let $\Delta^{(i)} = (0, \ldots, 1, \ldots, 0) \in \mathbb{F}_2^n$, where the 1 is in position i. Thus if f is an n-variable boolean function,

$$(D_i f)(x) = f(x + \Delta^{(i)}) + f(x)$$

for all $x \in \mathbb{F}_2^n$.

- What is $D_i D_i f$, for any function f?

  (A) 0 (B) 1 (C) $D_i f$ (D) depends on f

  You can check this by a calculation like the one just done. It also follows from Lemma 3.14(a), next slide, using that each boolean monomial has x_i at most once. Thie first part of the lemma also gives another proof that $D_i D_j f = D_j D_i f$.

Coefficient Formula

Given $I = \{i_1, \ldots, i_r\} \subseteq \{0, 1, \ldots, n-1\}$, define

$$D_I = D_{i_1} \ldots D_{i_r}.$$

(By the previous quiz, this is well-defined, e.g. $D_{\{0,2\}}$ can be read as either $D_0 D_2$ or $D_2 D_0$, and $D_{\{0,1,2\}} = D_0 D_1 D_2 = D_0 D_2 D_1 = \ldots$.)

Reminder of notation: $\{0, 2, 3\} \backslash \{2, 4\} = \{0, 3\}$.

Lemma 3.14

Let $J \subseteq \{0, 1, \ldots, n-1\}$.

(a) *If $i \in \{0, 1, \ldots, n-1\}$ then*

$$D_i x_J = \begin{cases} 0 & \text{if } i \notin J \\ J \backslash \{i\} & \text{if } i \in J. \end{cases}$$

(b) *Let $I \subseteq \{0, 1, \ldots, n-1\}$. Then*

$$D_I x_J = \begin{cases} 0 & \text{if } I \not\subseteq J \\ J \backslash I & \text{if } I \subseteq J. \end{cases}$$

Coefficient Formula

Reminder of notation: $\{0,2,3\}\backslash\{2,4\} = \{0,3\}$.

Lemma 3.14

Let $J \subseteq \{0,1,\ldots,n-1\}$.

(a) *If $i \in \{0,1,\ldots,n-1\}$ then*

$$D_i x_J = \begin{cases} 0 & \text{if } i \notin J \\ J\backslash\{i\} & \text{if } i \in J. \end{cases}$$

(b) *Let $I \subseteq \{0,1,\ldots,n-1\}$. Then*

$$D_I x_J = \begin{cases} 0 & \text{if } I \not\subseteq J \\ J\backslash I & \text{if } I \subseteq J. \end{cases}$$

Proposition 3.15

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be an n-variable boolean function. Then

$$[x_I]f = \sum f(z_0,\ldots,z_{n-1})$$

where the sum is over all $z_0,\ldots,z_{n-1} \in \{0,1\}$ such that $\{j : z_j = 1\} \subseteq I$.

See the printed notes for an outline of my preferred proof: you may be able to guess it from Lemma 3.14(b).

§4 The Discrete Fourier Transform

Preliminaries 4.1

It will be very helpful if you review the definition of vector spaces and inner products. If you know what it means to say that $u, v, w \in \mathbb{R}^3$ is an *orthonormal* basis of the vector space $\mathbb{R}^3$ with respect to the inner product $\langle -, - \rangle$ defined by

$$\big\langle (x_0, x_1, x_2), (y_0, y_1, y_2) \big\rangle = x_0 y_0 + x_1 y_1 + x_2 y_2$$

(this is the usual dot-product), and why it follows that

$$x = \langle x, u \rangle u + \langle x, v \rangle v + \langle x, w \rangle w$$

for any $x \in \mathbb{R}^3$, then the proof of Theorem 4.7 should seem easier and more motivated to you.

Quiz on the Dot Product on $\mathbb{R}^3$

Let $(\alpha, \beta, \gamma) \in \mathbb{R}^3$. What is

- $\langle (1,1,1), (\alpha, \beta, \gamma) \rangle$?

  (A) 0 (B) α (C) $\alpha + \beta + \gamma$ (D) $\alpha + \gamma$

True or false?

- $(1,1,1), (1,-1,0), (-1,-1,2)$ is a basis of $\mathbb{R}^3$.

  (A) False (B) True
- $(1,1,1), (1,-1,0), (-1,-1,2)$ is an orthogonal basis of $\mathbb{R}^3$, i.e. the dot product of any two distinct basis vectors is 0.

  (A) False (B) True
- $(1,1,1), (1,-1,0), (-1,-1,2)$ is an orthonormal basis of $\mathbb{R}^3$.

  (A) False (B) True
- $\frac{1}{\sqrt{3}}(1,1,1), \frac{1}{\sqrt{2}}(1,-1,0), \frac{1}{\sqrt{6}}(-1,-1,2)$ is an orthonormal basis of $\mathbb{R}^3$.

  (A) False (B) True

Quiz on the Dot Product on $\mathbb{R}^3$

Let $(\alpha, \beta, \gamma) \in \mathbb{R}^3$. What is

- $\langle (1,1,1), (\alpha, \beta, \gamma) \rangle$?

  (A) 0 (B) α (C) $\alpha + \beta + \gamma$ (D) $\alpha + \gamma$

True or false?

- $(1,1,1), (1,-1,0), (-1,-1,2)$ is a basis of $\mathbb{R}^3$.

  (A) False (B) True
- $(1,1,1), (1,-1,0), (-1,-1,2)$ is an orthogonal basis of $\mathbb{R}^3$, i.e. the dot product of any two distinct basis vectors is 0.

  (A) False (B) True
- $(1,1,1), (1,-1,0), (-1,-1,2)$ is an orthonormal basis of $\mathbb{R}^3$.

  (A) False (B) True
- $\frac{1}{\sqrt{3}}(1,1,1), \frac{1}{\sqrt{2}}(1,-1,0), \frac{1}{\sqrt{6}}(-1,-1,2)$ is an orthonormal basis of $\mathbb{R}^3$.

  (A) False (B) True

Quiz on the Dot Product on $\mathbb{R}^3$

Let $(\alpha, \beta, \gamma) \in \mathbb{R}^3$. What is

- $\langle (1,1,1), (\alpha, \beta, \gamma) \rangle$?

  (A) 0 (B) α (C) $\alpha + \beta + \gamma$ (D) $\alpha + \gamma$

True or false?

- $(1,1,1), (1,-1,0), (-1,-1,2)$ is a basis of $\mathbb{R}^3$.

  (A) False (B) True
- $(1,1,1), (1,-1,0), (-1,-1,2)$ is an orthogonal basis of $\mathbb{R}^3$, i.e. the dot product of any two distinct basis vectors is 0.

  (A) False (B) True
- $(1,1,1), (1,-1,0), (-1,-1,2)$ is an orthonormal basis of $\mathbb{R}^3$.

  (A) False (B) True
- $\frac{1}{\sqrt{3}}(1,1,1), \frac{1}{\sqrt{2}}(1,-1,0), \frac{1}{\sqrt{6}}(-1,-1,2)$ is an orthonormal basis of $\mathbb{R}^3$.

  (A) False (B) True

Quiz on the Dot Product on $\mathbb{R}^3$

Let $(\alpha, \beta, \gamma) \in \mathbb{R}^3$. What is

- $\langle (1,1,1), (\alpha, \beta, \gamma) \rangle$?

  (A) 0 (B) α (C) $\alpha + \beta + \gamma$ (D) $\alpha + \gamma$

True or false?

- $(1,1,1), (1,-1,0), (-1,-1,2)$ is a basis of $\mathbb{R}^3$.

  (A) False (B) True
- $(1,1,1), (1,-1,0), (-1,-1,2)$ is an orthogonal basis of $\mathbb{R}^3$, i.e. the dot product of any two distinct basis vectors is 0.

  (A) False (B) True
- $(1,1,1), (1,-1,0), (-1,-1,2)$ is an orthonormal basis of $\mathbb{R}^3$.

  (A) False (B) True
- $\frac{1}{\sqrt{3}}(1,1,1), \frac{1}{\sqrt{2}}(1,-1,0), \frac{1}{\sqrt{6}}(-1,-1,2)$ is an orthonormal basis of $\mathbb{R}^3$.

  (A) False (B) True

Quiz on the Dot Product on $\mathbb{R}^3$

Let $(\alpha, \beta, \gamma) \in \mathbb{R}^3$. What is

- $\langle (1,1,1), (\alpha, \beta, \gamma) \rangle$?

  (A) 0 (B) α (C) $\alpha + \beta + \gamma$ (D) $\alpha + \gamma$

True or false?

- $(1,1,1), (1,-1,0), (-1,-1,2)$ is a basis of $\mathbb{R}^3$.

  (A) False (B) True
- $(1,1,1), (1,-1,0), (-1,-1,2)$ is an orthogonal basis of $\mathbb{R}^3$, i.e. the dot product of any two distinct basis vectors is 0.

  (A) False (B) True
- $(1,1,1), (1,-1,0), (-1,-1,2)$ is an orthonormal basis of $\mathbb{R}^3$.

  (A) False (B) True
- $\frac{1}{\sqrt{3}}(1,1,1), \frac{1}{\sqrt{2}}(1,-1,0), \frac{1}{\sqrt{6}}(-1,-1,2)$ is an orthonormal basis of $\mathbb{R}^3$.

  (A) False (B) True
- When (α, β, γ) is written as a linear combination of the basis vectors in this orthonormal basis the coefficient of $(1,-1,0)$ is $\frac{1}{\sqrt{2}}(\alpha - \beta)$.

  (A) False (B) True

Quiz on the Dot Product on $\mathbb{R}^3$

Let $(\alpha, \beta, \gamma) \in \mathbb{R}^3$. What is

- $\langle (1,1,1), (\alpha, \beta, \gamma) \rangle$?

  (A) 0 (B) α (C) $\alpha + \beta + \gamma$ (D) $\alpha + \gamma$

True or false?

- $(1,1,1), (1,-1,0), (-1,-1,2)$ is a basis of $\mathbb{R}^3$.

  (A) False (B) True
- $(1,1,1), (1,-1,0), (-1,-1,2)$ is an orthogonal basis of $\mathbb{R}^3$, i.e. the dot product of any two distinct basis vectors is 0.

  (A) False (B) True
- $(1,1,1), (1,-1,0), (-1,-1,2)$ is an orthonormal basis of $\mathbb{R}^3$.

  (A) False (B) True
- $\frac{1}{\sqrt{3}}(1,1,1), \frac{1}{\sqrt{2}}(1,-1,0), \frac{1}{\sqrt{6}}(-1,-1,2)$ is an orthonormal basis of $\mathbb{R}^3$.

  (A) False (B) True
- When (α, β, γ) is written as a linear combination of the basis vectors in this orthonormal basis the coefficient of $(1,-1,0)$ is $\frac{1}{\sqrt{2}}(\alpha - \beta)$.

  (A) False (B) True

Quiz on the Dot Product on $\mathbb{R}^3$

Let $(\alpha, \beta, \gamma) \in \mathbb{R}^3$. What is

- $\langle (1,1,1), (\alpha, \beta, \gamma) \rangle$?

  (A) 0 (B) α (C) $\alpha + \beta + \gamma$ (D) $\alpha + \gamma$

True or false?

- $(1,1,1), (1,-1,0), (-1,-1,2)$ is a basis of $\mathbb{R}^3$.

  (A) False (B) True
- $(1,1,1), (1,-1,0), (-1,-1,2)$ is an orthogonal basis of $\mathbb{R}^3$, i.e. the dot product of any two distinct basis vectors is 0.

  (A) False (B) True
- $(1,1,1), (1,-1,0), (-1,-1,2)$ is an orthonormal basis of $\mathbb{R}^3$.

  (A) False (B) True
- $\frac{1}{\sqrt{3}}(1,1,1), \frac{1}{\sqrt{2}}(1,-1,0), \frac{1}{\sqrt{6}}(-1,-1,2)$ is an orthonormal basis of $\mathbb{R}^3$.

  (A) False (B) True

  If $u = \frac{1}{\sqrt{3}}(1,1,1)$, $v = \frac{1}{\sqrt{2}}(1,-1,0)$ and $w = \frac{1}{\sqrt{6}}(-1,-1,2)$ then in fact

$$(\alpha, \beta, \gamma) = \frac{1}{\sqrt{3}}(\alpha+\beta+\gamma)u + \frac{1}{\sqrt{2}}(\alpha-\beta)v + \frac{1}{\sqrt{6}}(-\alpha-\beta+2\gamma)w.$$

Correlations

Given $x \in \mathbb{F}_2$ we define $(-1)^x$ by regarding x as an ordinary integer. Thus $(-1)^0 = 1$ and $(-1)^1 = -1$. Given an n-variable boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ we define $(-1)^f : \mathbb{F}_2^n \to \{-1, 1\}$ by $(-1)^f(x) = (-1)^{f(x)}$.

Definition 4.2

Let $f, g : \mathbb{F}_2^n \to \mathbb{F}$ be boolean functions. We define the *correlation* between f and g by

$$\mathrm{corr}(f, g) = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} (-1)^{g(x)}.$$

The summand $(-1)^{f(x)}(-1)^{g(x)}$ is 1 when $f(x) = g(x)$ and -1 when $f(x) = -g(x)$. Hence

$$\mathrm{corr}(f, g) = \frac{c_{\mathrm{same}} - c_{\mathrm{diff}}}{2^n}$$

where

$$c_{\mathrm{same}} = \left|\{x \in \mathbb{F}_2^n : f(x) = g(x)\}\right|, \; c_{\mathrm{diff}} = \left|\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}\right|.$$

Linear Functions

Given $T \subseteq \{0, 1, \ldots, n-1\}$, define $L_T : \mathbb{F}_2^n \to \mathbb{F}_2$ by

$$L_T(x) = \sum_{t \in T} x_t.$$

For example, $L_{\{i\}}(x_0, x_1, \ldots, x_{n-1}) = x_i$ returns the entry in position i and $L_\varnothing(x) = 0$ is the zero function.

Exercise 4.3

(i) Compute the correlation between the Toffoli function (see Example 3.6) and each of the functions $L_\varnothing$, $L_{\{0\}}$, $L_{\{2\}}$.

(ii) In general, when is a 3-variable boolean function uncorrelated with the zero function?

Linear Functions and Correlations

Given $S, T \subseteq \{0, 1, \ldots, n-1\}$, define

$$S \triangle T = \{u : u \in S \cup T, u \notin S \cap T\}.$$

For instance $\{1, 2\} \triangle \{0, 2, 3\} = \{0, 1, 3\}$.

Lemma 4.4

(a) *The linear functions* $\mathbb{F}_2^n \to \mathbb{F}$ *are precisely the* $L_T : \mathbb{F}_2^n \to \mathbb{F}_2$ *for* $T \subseteq \{0, 1, \ldots, n-1\}$.

(b) *We have* $L_S + L_T = L_{S \triangle T}$ *for all* $S, T \subseteq \{0, 1, \ldots, n-1\}$.

(c) $L_\varnothing$ *is the zero function.*

(d) *If* $T \subseteq \{0, 1, \ldots, n-1\}$ *and* $T \neq \varnothing$ *then* $\mathrm{corr}(L_T, 0) = 0$

(e) *If* $S, T \subseteq \{0, 1, \ldots, n-1\}$ *then*

$$\mathrm{corr}(L_S, L_T) = \begin{cases} 1 & \text{if } S = T \\ 0 & \text{otherwise.} \end{cases}$$

The symmetric difference appears again on Question 6(b) on Problem Sheet 3.

Majority Vote as a 'Combination' of Linear Functions

Recall that if $T \subseteq \{0, 1, \ldots, n-1\}$ then $L_T : \mathbb{F}_2^n \to \mathbb{F}_2$ is the linear n-variable boolean function defined by $L_T(x) = \sum_{t \in T} x_t$.

- The 3-variable boolean function $L_{\{1,2\}} + L_{\{1,3\}}$ is linear?

(A) False (B) True

Example 4.5

Let $\mathrm{maj} : \mathbb{F}_2^3 \to \mathbb{F}_2$ be the majority vote function from Exercise .

$$\mathrm{corr}(\mathrm{maj}, L_T) = \begin{cases} \frac{1}{2} & \text{if } T = \{0\}, \{1\}, \{2\} \\ -\frac{1}{2} & \text{if } T = \{0, 1, 2\} \\ 0 & \text{otherwise.} \end{cases}$$

Majority Vote as a 'Combination' of Linear Functions

Recall that if $T \subseteq \{0, 1, \ldots, n-1\}$ then $L_T : \mathbb{F}_2^n \to \mathbb{F}_2$ is the linear n-variable boolean function defined by $L_T(x) = \sum_{t \in T} x_t$.

- The 3-variable boolean function $L_{\{1,2\}} + L_{\{1,3\}}$ is linear?

  (A) False (B) True

- Since it is linear, it must be equal to some L_T by Lemma 4.4. What is T?

  (A) $\{1, 2\}$ (B) $\{1, 2, 3\}$ (C) $\{2, 3\}$ (D) $\varnothing$

Example 4.5

Let $\mathrm{maj} : \mathbb{F}_2^3 \to \mathbb{F}_2$ be the majority vote function from Exercise .

$$\mathrm{corr}(\mathrm{maj}, L_T) = \begin{cases} \frac{1}{2} & \text{if } T = \{0\}, \{1\}, \{2\} \\ -\frac{1}{2} & \text{if } T = \{0, 1, 2\} \\ 0 & \text{otherwise.} \end{cases}$$

Moreover

$$(-1)^{\mathrm{maj}(x)} = \tfrac{1}{2}(-1)^{L_{\{1\}}(x)} + \tfrac{1}{2}(-1)^{L_{\{2\}}(x)} + \tfrac{1}{2}(-1)^{L_{\{3\}}(x)} + \tfrac{1}{2}(-1)^{L_{\{1,2,3\}}(x)}$$

So although majority vote is not linear, $(-1)^{\mathrm{maj}}$ is equal to a linear combination of the $(-1)^{L_T}$ functions.

Majority Vote as a 'Combination' of Linear Functions

Recall that if $T \subseteq \{0, 1, \ldots, n-1\}$ then $L_T : \mathbb{F}_2^n \to \mathbb{F}_2$ is the linear n-variable boolean function defined by $L_T(x) = \sum_{t \in T} x_t$.

- The 3-variable boolean function $L_{\{1,2\}} + L_{\{1,3\}}$ is linear?

  (A) False (B) True

- Since it is linear, it must be equal to some L_T by Lemma 4.4. What is T?

  (A) $\{1, 2\}$ (B) $\{1, 2, 3\}$ (C) $\{2, 3\}$ (D) $\varnothing$

Example 4.5

Let $\mathrm{maj} : \mathbb{F}_2^3 \to \mathbb{F}_2$ be the majority vote function from Exercise .

$$\mathrm{corr}(\mathrm{maj}, L_T) = \begin{cases} \frac{1}{2} & \text{if } T = \{0\}, \{1\}, \{2\} \\ -\frac{1}{2} & \text{if } T = \{0, 1, 2\} \\ 0 & \text{otherwise.} \end{cases}$$

Moreover

$$(-1)^{\mathrm{maj}(x)} = \tfrac{1}{2}(-1)^{L_{\{1\}}(x)} + \tfrac{1}{2}(-1)^{L_{\{2\}}(x)} + \tfrac{1}{2}(-1)^{L_{\{3\}}(x)} + \tfrac{1}{2}(-1)^{L_{\{1,2,3\}}(x)}$$

So although majority vote is not linear, $(-1)^{\mathrm{maj}}$ is equal to a linear combination of the $(-1)^{L_T}$ functions.

Inner Product on Real-Valued Functions on $\mathbb{F}_2^n$

We define an inner product on the vector space W of functions $\mathbb{F}_2^n \to \mathbb{R}$ by

$$\langle \theta, \phi \rangle = \frac{1}{2^n} \sum_{x \in 2^n} \theta(x)\phi(x).$$

If f and g are n-variable boolean functions then critically

$$\langle (-1)^f, (-1)^g \rangle = \mathrm{corr}(f, g). \qquad (\star)$$

Exercise 4.6

(i) Let $\theta \in W$. Check that, as required for an inner product, $\langle \theta, \theta \rangle \geq 0$ and that $\langle \theta, \theta \rangle = 0$ if and only if $\theta(x) = 0$ for all $x \in \mathbb{F}_2^n$.

(ii) Show that if $n = 2$ then W is 4-dimensional. What is $\dim W$ in general?

Inner Product on Real-Valued Functions on $\mathbb{F}_2^n$

We define an inner product on the vector space W of functions $\mathbb{F}_2^n \to \mathbb{R}$ by

$$\langle \theta, \phi \rangle = \frac{1}{2^n} \sum_{x \in 2^n} \theta(x)\phi(x).$$

If f and g are n-variable boolean functions then critically

$$\langle (-1)^f, (-1)^g \rangle = \mathrm{corr}(f, g). \qquad (\star)$$

Exercise 4.6

(i) Let $\theta \in W$. Check that, as required for an inner product, $\langle \theta, \theta \rangle \geq 0$ and that $\langle \theta, \theta \rangle = 0$ if and only if $\theta(x) = 0$ for all $x \in \mathbb{F}_2^n$.

(ii) Show that if $n = 2$ then W is 4-dimensional. What is $\dim W$ in general?

Writing functions $f \in W$ like columns of truth tables $\begin{pmatrix} f(0,0) \\ f(0,1) \\ f(1,0) \\ f(1,1) \end{pmatrix}$, we have

$$(-1)^{L_\varnothing} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \quad \text{and} \quad (-1)^{L_{\{1\}}} = \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix} \quad \text{and so on.}$$

Reminder of Inner Product Spaces

- Any orthonormal set is linearly independent: for instance, with three orthonormal vectors u, v, w, if $\lambda u + \mu v + \nu w = 0$ then taking the inner product with u we get

$$0 = \langle 0, u \rangle = \langle \lambda u + \mu v + \nu w, u \rangle = \lambda.$$

- If $x = \lambda u + \mu v + \nu w$ where u, v, w are orthonormal then $\langle x, x \rangle = \lambda^2 + \mu^2 + \nu^2$.

For instance, using the orthonormal basis $u = \frac{1}{\sqrt{3}}(1,1,1)$, $v = \frac{1}{\sqrt{2}}(1,-1,0)$ and $w = \frac{1}{\sqrt{6}}(-1,-1,2)$ from earlier, we saw that

$$\begin{aligned}(\alpha,\beta,\gamma) &= \langle (\alpha,\beta,\gamma), u\rangle u + \langle (\alpha,\beta,\gamma), v\rangle v + \langle (\alpha,\beta,\gamma), w\rangle w \\ &= \frac{1}{\sqrt{3}}(\alpha+\beta+\gamma)u + \frac{1}{\sqrt{2}}(\alpha-\beta)v + \frac{1}{\sqrt{6}}(-\alpha-\beta+2\gamma)w.\end{aligned}$$

Correspondingly, check that $\langle (\alpha,\beta,\gamma), (\alpha,\beta,\gamma)\rangle$ is

$$\frac{1}{3}(\alpha+\beta+\gamma)^2 + \frac{1}{2}(\alpha-\beta)^2 + \frac{1}{6}(-\alpha-\beta+2\gamma)^2.$$

Discrete Fourier Transform

The inner product on the vector space W of functions $\mathbb{F}_2^n \to \mathbb{R}$ is defined by

$$\langle \theta, \phi \rangle = \frac{1}{2^n} \sum_{x \in 2^n} \theta(x)\phi(x).$$

We saw that $\langle (-1)^f, (-1)^g \rangle = \mathrm{corr}(f, g)$ for n-variable boolean functions f and g.

Theorem 4.7 (Discrete Fourier Transform)

(a) *The functions* $(-1)^{L_T}$ *for* $T \subseteq \{0, 1, \ldots, n-1\}$ *are an orthonormal basis for the vector space* W *of functions* $\mathbb{F}_2^n \to \mathbb{R}$.

(b) *Let* $\theta : \mathbb{F}_2^n \to \mathbb{R}$. *Then*

$$\theta = \sum_{T \subseteq \{0,1,\ldots,n-1\}} \langle \theta, (-1)^{L_T} \rangle (-1)^{L_T}.$$

(c) *Let* $f : \mathbb{F}_2^n \to \mathbb{F}_2$ *be a boolean function. Then*

$$(-1)^f = \sum_{T \subseteq \{0,1,\ldots,n-1\}} \mathrm{corr}(f, L_T)(-1)^{L_T}.$$

Parseval's Theorem

Corollary 4.8

Let f be an n-variable boolean function. Then

$$\sum_{T\subseteq\{0,1,\ldots,n-1\}} \mathrm{corr}(f, L_T)^2 = 1.$$

Since there are 2^n linear functions (corresponding to the 2^n subsets of $\{0, 1, \ldots, n-1\}$), it follows that any n-variable boolean function f has a squared correlation of at least $1/2^n$.

Example 4.9

(1) Let $f(x_0, x_1, x_2) = x_0x_1x_2$. We have $\mathrm{corr}(f, L_\varnothing) = \frac{3}{4}$, $\mathrm{corr}(f, L_{\{0\}}) = \frac{1}{4}$, $\mathrm{corr}(f, L_{\{0,1\}}) = -\frac{1}{4}$ and $\mathrm{corr}(f, L_{\{0,1,2\}}) = \frac{1}{4}$. By Theorem 4.7(c) and symmetry, the Discrete Fourier Transform of f is

$$(-1)^f = \frac{3}{4} + \frac{1}{4} \sum_{\substack{T\subseteq\{0,1,2\}\\ T\neq\varnothing}} (-1)^{|T|-1}(-1)^{L_T}.$$

We will check Parseval's Theorem holds.

Example 4.9 [continued]

(2) *Exercise:* Consider the 2-variable boolean function $f(x_0, x_1) = x_0x_1$. Find its correlations with the four linear functions $L_\varnothing(x_0, x_1) = 1$, $L_{\{0\}}(x_0, x_1) = x_0$, $L_{\{1\}}(x_0, x_1) = x_1$, $L_{\{0,1\}}(x_0, x_1) = x_1 + x_2$ and deduce that

$$(-1)^{x_0x_1} = \tfrac{1}{2}(-1)^{L_\varnothing} + \tfrac{1}{2}(-1)^{L_{\{0\}}} + \tfrac{1}{2}(-1)^{L_{\{1\}}} - \tfrac{1}{2}(-1)^{L_{\{0,1\}}}$$

(3) Let $b(x_0, x_1, x_2, x_3) = x_0x_2 + x_1x_3$. The MATHEMATICA notebook `BooleanCorrelations.nb` on Moodle shows that $\mathrm{corr}(b, L_T) = \pm\frac{1}{4}$ for every $T \subseteq \{0, 1, 2, 3\}$.

Out[•]//TableForm=

{}	{0}	{1}	{2}	{3}	{0, 1}	{0, 2}	{0, 3}
$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$

By the remark following Corollary 4.8, this function achieves the cryptographic ideal of having all correlations as small (in absolute value) as possible.

Bent Functions

An n-variable boolean function such as b where the correlations all have absolute value $1/\sqrt{2^n}$ is called a *bent function*.

Exercise 4.10

(i) Show that if there is an n-variable bent function then n is even. [*Hint:* correlations are rational numbers.]

(ii) What is the correlation between a bent function and the zero function $L_\varnothing$?

(iii) Can you find some more 4-variable bent functions? [*Hint:* the MATHEMATICA notebook `BooleanCorrelations.nb` will help you search!]

Since a bent function b has a slight bias towards 0 if $\mathrm{corr}(f, L_\varnothing) = 1/\sqrt{2^n}$, and towards 1 if $\mathrm{corr}(f, L_\varnothing) = -1/\sqrt{2^n}$, they are not used as cryptographic primitives without some tweaking. The block cipher CAST makes uses of modified bent-functions.

Piling-Up Lemma

Lemma 4.11 (Piling-up Lemma)

Let f be an m-variable boolean function of $u_0, \ldots, u_{m-1}$ and let g be an n-variable boolean function of $v_0, \ldots, v_{n-1}$. Define $f+g$ by

$$(f+g)(u_0, \ldots, u_{m-1}, v_0, \ldots, v_{n-1}) = f(u_0, \ldots, u_{m-1}) + g(v_0, \ldots, v_{n-1}).$$

Given $S \subseteq \{0, \ldots, m-1\}$ and $T \subseteq \{0, \ldots, n-1\}$, let $L_{(S,T)}(u, v) = L_S(u) + L_T(v)$. The $L_{(S,T)}$ are all linear functions of the $m+n$ variables and

$$\mathrm{corr}(f+g, L_{(S,T)}) = \mathrm{corr}(f, L_S)\,\mathrm{corr}(g, L_T).$$

For instance the Piling-up Lemma implies that

$$x_0y_0 + \cdots + x_{m-1}y_{m-1}$$

is a bent function for all m, generalizing Example 4.9. [*Hint:* apply it repeatedly. To get the correlations for $x_0y_0 + x_1y_1$ take $u_0 = x_0$, $u_1 = y_0$, $v_0 = x_1$ and $v_1 = y_1$ and use Example 4.9(2).]

§5 Keystreams and annihilators

In Example 8.2 of the main course we will take the sum of the keystream of the LFSR of width 4 and taps $\{3, 4\}$ and the keystream of the LFSR of width 3 with taps $\{2, 3\}$.

```
In[261]:= Keystream[{3, 4}, {0, 0, 0, 1}, 20]

Out[261]= {0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0}

In[262]:= Keystream[{2, 3}, {0, 0, 1}, 20]

Out[262]= {0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1}

In[263]:= Keystream[{3, 4}, {0, 0, 0, 1}, 20] +
            Keystream[{2, 3}, {0, 0, 1}, 20] // ModTwo

Out[263]= {0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1}

In[265]:= Keystream[{2, 4, 5, 7}, {0, 0, 1, 1, 1, 1, 0}, 20]

Out[265]= {0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1}
```

§5 Keystreams and annihilators

In Example 8.2 of the main course we will take the sum of the keystream of the LFSR of width 4 and taps $\{3, 4\}$ and the keystream of the LFSR of width 3 with taps $\{2, 3\}$.

Perhaps surprisingly, the sum is a keystream of the LFSR of width 7 with taps $\{2, 4, 5, 7\}$. The main goal in this section is to prove Corollary 5.5 that explains why these taps are the non-zero powers of z appears in the product

$$(1 + z^3 + z^4)(1 + z^2 + z^3) = 1 + z^2 + z^4 + z^5 + z^7,$$

computed as usual working modulo 2.

Definition 5.1

The *power series* representing a keystream $k_0 k_1 k_2 \ldots$ is $k_0 + k_1 z + k_2 z^2 + \cdots$.

Example 5.2

The power series $\kappa(z)$ representing the keystream of the LFSR F of width 3 and taps $\{2, 3\}$ with key 110 is

$$1+z+z^4+z^6+z^7+z^8+z^{11}+z^{13}+z^{14}+z^{15}+\cdots \longleftrightarrow 110010111001011\ldots$$

(a) Observe that the coefficient of z^m in $(1 + z^7)\kappa(X)$ comes from z^m and z^{m-7}, and so is $k_m + k_{m-7}$, for all $m \geq 7$. Since the keystream has period 7, $k_m = k_{m-7}$ and hence the coefficient of x^s in $(1 + z^7)\kappa(X)$ is zero for $s \geq 7$. Thus $(1 + z^7)\kappa(z)$ is a polynomial. Explicitly,

$$(1 + z^7)\kappa(z) = 1 + z + z^4 + z^6.$$

(b) *Exercise:* show using the method on the slides for (a) that $(1 + z^2 + z^3)\kappa(z)$ is a polynomial.

(c) *Exercise:* what is the product of the power series for the keystream $1011100\ldots$ produced by F and $1 + z^2 + z^3$?

(d) Warning example. The product of $\kappa(z)$ with $1 + z$ is

$$1+z^2+z^4+z^5+z^6+z^9+z^{11}+z^{12}+z^{13}+\cdots \longleftrightarrow 1010111001011100\ldots$$

Exercise: is the right-hand side a keystream of F?

Example 5.2

The power series $\kappa(z)$ representing the keystream of the LFSR F of width 3 and taps $\{2, 3\}$ with key 110 is

$$1+z+z^4+z^6+z^7+z^8+z^{11}+z^{13}+z^{14}+z^{15}+\cdots \longleftrightarrow 110010111001011\ldots$$

(a) Observe that the coefficient of z^m in $(1+z^7)\kappa(X)$ comes from z^m and z^{m-7}, and so is $k_m + k_{m-7}$, for all $m \geq 7$. Since the keystream has period 7, $k_m = k_{m-7}$ and hence the coefficient of x^s in $(1+z^7)\kappa(X)$ is zero for $s \geq 7$. Thus $(1+z^7)\kappa(z)$ is a polynomial. Explicitly,

$$(1+z^7)\kappa(z) = 1 + z + z^4 + z^6.$$

(b) *Exercise:* show using the method on the slides for (a) that $(1+z^2+z^3)\kappa(z)$ is a polynomial.

(c)

```
In[268]:= KeystreamToPolynomial[{1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0}] * (1 + z^2 + z^3) // Expand //
          PMod

Out[268]= 1 + z^14
```

(d) Warning example. The product of $\kappa(z)$ with $1+z$ is

$$1+z^2+z^4+z^5+z^6+z^9+z^{11}+z^{12}+z^{13}+\cdots \longleftrightarrow 1010111001011100\ldots$$

Exercise: is the right-hand side a keystream of F?

Tapping Polynomial

Motivated by (b), we define the *feedback polynomial* of a LFSR with taps T to be

$$g_T(z) = 1 + \sum_{t \in T} z^t$$

and make the following definition.

Definition 5.3

Let $\kappa(z)$ be an infinite power series with coefficients in $\mathbb{F}_2$. Let $g(z)$ be a polynomial. We say that $g(z)$ *annihilates* $\kappa(z)$ if $g(z)\kappa(z)$ is a polynomial.

For example, we have seen that if

$$\kappa(z) = 1 + z + z^4 + z^6 + z^7 + z^8 + z^{11} + z^{13} + \cdots$$

is the power series corresponding to a keystream of the LFSR of width 3 and period 7 with taps $\{2, 3\}$ then $\kappa(z)$ is annihilated by $1 + z^7$ and also by $1 + z^2 + z^3$, but not by $1 + z$.

Algebra Can be Powerful!

Definition 5.3

Let $\kappa(z)$ be an infinite power series with coefficients in $\mathbb{F}_2$. Let $g(z)$ be a polynomial. We say that $g(z)$ *annihilates* $\kappa(z)$ if $g(z)\kappa(z)$ is a polynomial.

Lemma 5.4

Let $u_0 u_1 u_2 \ldots$ *be a keystream and let*

$$\kappa(z) = u_0 + u_1 z + u_2 z^2 + \cdots$$

be the corresponding power series. Let $T \subseteq \{1, \ldots, \ell\}$. *The polynomial* $g_T(z)$ *annihilates* $\kappa(z)$ *with* $\deg g_T(z)\kappa(z) < \ell$ *if and only if* $u_0 u_1 u_2 \ldots$ *is a keystream of an LFSR with taps* T *and width* ℓ.

Algebra Can be Powerful!

Lemma 5.4

Let $u_0 u_1 u_2 \ldots$ be a keystream and let

$$\kappa(z) = u_0 + u_1 z + u_2 z^2 + \cdots$$

be the corresponding power series. Let $T \subseteq \{1, \ldots, \ell\}$. The polynomial $g_T(z)$ annihilates $\kappa(z)$ with $\deg g_T(z)\kappa(z) < \ell$ if and only if $u_0 u_1 u_2 \ldots$ is a keystream of an LFSR with taps T and width ℓ.

Proof.

Let $s \geq \max T$. The coefficient of z^s in $(1 + \sum_{t \in T} z^t)\kappa(z)$ is the sum of u_s (from multiplying by 1) and $\sum_{t \in T} u_{s-t}$ (from multiplying by $\sum_{t \in T} z^t$). Hence it is $u_s + \sum_{t \in T} u_{s-t}$. This is zero for all $s \geq \ell$ if and only if $u_0 u_1 u_2 \ldots$ is a keystream of the LFSR with taps T and width ℓ. □

Algebra Can be Powerful!

Lemma 5.4

Let $u_0 u_1 u_2 \ldots$ be a keystream and let

$$\kappa(z) = u_0 + u_1 z + u_2 z^2 + \cdots$$

be the corresponding power series. Let $T \subseteq \{1, \ldots, \ell\}$. The polynomial $g_T(z)$ annihilates $\kappa(z)$ with $\deg g_T(z)\kappa(z) < \ell$ if and only if $u_0 u_1 u_2 \ldots$ is a keystream of an LFSR with taps T and width ℓ.

The keystream 0010111 0010111 ... is produced by the LFSR of width 3 and taps $\{2, 3\}$.

- What are the taps of the smallest width LFSR generating 00010111 0010111 ...? Note extra **0** at the start.

  (A) $\{1, 2\}$ (B) $\{1, 3\}$ (C) $\{2, 3\}$ (D) $\{1, 2, 3\}$
- What is the width of this LFSR?

  (A) 2 (B) 3 (C) 4 (D) > 4

This shows we may need to take $\ell > \max T$. (This was also seen in Example 5.2(d).) For a simpler example, the keystream that is all zero except in position 2, i.e. 001000 ... is the output of an LFSR of width 3 with empty taps, but no LFSR of smaller width.

Algebra Can be Powerful!

Lemma 5.4

Let $u_0 u_1 u_2 \ldots$ be a keystream and let

$$\kappa(z) = u_0 + u_1 z + u_2 z^2 + \cdots$$

be the corresponding power series. Let $T \subseteq \{1, \ldots, \ell\}$. The polynomial $g_T(z)$ annihilates $\kappa(z)$ with $\deg g_T(z)\kappa(z) < \ell$ if and only if $u_0 u_1 u_2 \ldots$ is a keystream of an LFSR with taps T and width ℓ.

The keystream 0010111 0010111 ... is produced by the LFSR of width 3 and taps $\{2, 3\}$.

- What are the taps of the smallest width LFSR generating 00010111 0010111 ...? Note extra **0** at the start.

  (A) $\{1, 2\}$ (B) $\{1, 3\}$ (C) $\{2, 3\}$ (D) $\{1, 2, 3\}$
- What is the width of this LFSR?

  (A) 2 (B) 3 (C) 4 (D) > 4

This shows we may need to take $\ell > \max T$. (This was also seen in Example 5.2(d).) For a simpler example, the keystream that is all zero except in position 2, i.e. 001000 ... is the output of an LFSR of width 3 with empty taps, but no LFSR of smaller width.

Algebra Can be Powerful!

Lemma 5.4

Let $u_0 u_1 u_2 \ldots$ be a keystream and let

$$\kappa(z) = u_0 + u_1 z + u_2 z^2 + \cdots$$

be the corresponding power series. Let $T \subseteq \{1, \ldots, \ell\}$. The polynomial $g_T(z)$ annihilates $\kappa(z)$ with $\deg g_T(z)\kappa(z) < \ell$ if and only if $u_0 u_1 u_2 \ldots$ is a keystream of an LFSR with taps T and width ℓ.

The keystream 0010111 0010111 ... is produced by the LFSR of width 3 and taps $\{2, 3\}$.

- What are the taps of the smallest width LFSR generating 00010111 0010111 ...? Note extra **0** at the start.

  (A) $\{1, 2\}$ (B) $\{1, 3\}$ (C) $\{2, 3\}$ (D) $\{1, 2, 3\}$
- What is the width of this LFSR?

  (A) 2 (B) 3 (C) 4 (D) > 4

This shows we may need to take $\ell > \max T$. (This was also seen in Example 5.2(d).) For a simpler example, the keystream that is all zero except in position 2, i.e. 001000 ... is the output of an LFSR of width 3 with empty taps, but no LFSR of smaller width.

Question 4 on Problem Sheet 4

Corollary 5.5

Suppose that $k_0 k_1 k_2 \ldots$ is a keystream of an LFSR with taps T and width ℓ and $k'_0 k'_1 k'_2 \ldots$ is a keystream of an LFSR with taps T' and width ℓ'. Let $u_s = k_s + k'_s$ for each $s \in \mathbb{N}_0$. Then $u_0 u_1 u_2 \ldots$ is a keystream of the LFSR of width $\ell + \ell'$ with feedback polynomial $g_T(z) g_{T'}(z)$.

Determining Periods

Corollary 5.6

Let F be an invertible LFSR with taps T and let $m \in \mathbb{N}$. The following are equivalent:

(a) *every keystream of F has period dividing m;*

(b) *$1 + z^m$ annihilates every power series $\kappa(z)$ corresponding to a keystream of F and $(1 + z^m)\kappa(z)$ has degree $< m$;*

(c) *$g_T(z)$ divides $1 + z^m$.*

Moreover if m is the least number with any of these properties then m is the period of F and F has a keystream of period m.

Determining Periods

Corollary 5.6

Let F be an invertible LFSR with taps T and let $m \in \mathbb{N}$. The following are equivalent:

(a) *every keystream of F has period dividing m;*

(b) *$1 + z^m$ annihilates every power series $\kappa(z)$ corresponding to a keystream of F and $(1 + z^m)\kappa(z)$ has degree $< m$;*

(c) *$g_T(z)$ divides $1 + z^m$.*

Moreover if m is the least number with any of these properties then m is the period of F and F has a keystream of period m.

Lemma 5.4

Let $u_0 u_1 u_2 \ldots$ be a keystream and let

$$\kappa(z) = u_0 + u_1 z + u_2 z^2 + \cdots$$

be the corresponding power series. Let $T \subseteq \{1, \ldots, \ell\}$. The polynomial $g_T(z)$ annihilates $\kappa(z)$ with $\deg g_T(z)\kappa(z) < \ell$ if and only if $u_0 u_1 u_2 \ldots$ is a keystream of an LFSR with taps T and width ℓ.

Determining Periods

Corollary 5.6

Let F be an invertible LFSR with taps T and let $m \in \mathbb{N}$. The following are equivalent:

(a) *every keystream of F has period dividing m;*

(b) *$1 + z^m$ annihilates every power series $\kappa(z)$ corresponding to a keystream of F and $(1 + z^m)\kappa(z)$ has degree $< m$;*

(c) *$g_T(z)$ divides $1 + z^m$.*

Moreover if m is the least number with any of these properties then m is the period of F and F has a keystream of period m.

This improves on the corollary of (**VUP**) seen in the main course that the period of F is the lowest common multiple of the periods of the keystreams: by the final part, it is simply the maximum of the keystream periods.

Determining Periods

Corollary 5.6

Let F be an invertible LFSR with taps T and let $m \in \mathbb{N}$. The following are equivalent:

(a) *every keystream of F has period dividing m;*

(b) *$1 + z^m$ annihilates every power series $\kappa(z)$ corresponding to a keystream of F and $(1 + z^m)\kappa(z)$ has degree $< m$;*

(c) *$g_T(z)$ divides $1 + z^m$.*

Moreover if m is the least number with any of these properties then m is the period of F and F has a keystream of period m.

To work with Corollary 5.6, the following lemma is useful. Let $\mathrm{hcf}(d, e)$ denote the highest common factor of d, $e \in \mathbb{N}$.

Lemma 5.7

If a polynomial $g(z)$ divides $z^d + 1$ and $z^e + 1$ then it divides $z^{\mathrm{hcf}(d,e)} + 1$.

Example of Corollary 5.6 and Lemma 5.7

Example 5.8

The number $2^{13} - 1 = 8191$ is prime. The MATHEMATICA command `Factor[z^8191 + 1, Modulus -> 2]` reports that

$$z^{8191} + 1 = (1+z)(1+z+z^3+z^4+z^{13})(1+z+z^2+z^5+z^{13})\ldots.$$

(Here ... stands for 630 omitted factors all of degree 13.) The taps of the LFSR of width 13 with feedback polynomial $f(z) = 1 + z + z^3 + z^4 + z^{13}$ are $1, 3, 4, 13$. By Corollary 5.6, its period is the least m such that $f(z)$ divides $z^m + 1$. If $1 + z + z^3 + z^4 + z^{13}$ divides $z^e + 1$ with $e < 8191$ then, by Lemma 5.7, $1 + z + z^3 + z^4 + z^{13}$ divides $z^{\mathrm{hcf}(e,8191)} + 1 = z + 1$, a contradiction. Since $1 + z + z^3 + z^4 + z^{13}$ divides $z^{8191} + 1$, its period is 8191.

§6 The Berlekamp–Massey Algorithm

Example 6.1

The sum u of the keystreams of the LFSR with taps $\{3, 4\}$ and width 4 and the LFSR with taps $\{2, 3\}$ and width 3, using keys 0001 and 001, has period $15 \times 7 = 105$.

$$u_i = (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, \ldots)$$
$$0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

The output of the Berlekamp–Massey algorithm applied to the first n terms $u_0 \ldots u_{n-1}$ for $n \geq 6$ is below. No change for $n = 7, 8, 12$. (Ignore the column labelled m for the moment.)

n	width	feedback polynomial	taps	m
6	3	$1 + z$	$\{1\}$	2
9	4	$1 + z + z^4$	$\{1, 4\}$	6
10	6	$1 + z + z^3$	$\{1, 3\}$	9
11	6	$1 + z^2 + z^3 + z^5$	$\{2, 3, 5\}$	9
≥ 13	7	$1 + z^2 + z^4 + z^5 + z^7$	$\{2, 4, 5, 7\}$	12

Example 6.1 [continued]

Example 6.1

```
In[•]:= usEx61 := Keystream[{3, 4}, {0, 0, 0, 1}, 15] + Keystream[{2, 3}, {0, 0, 1}, 15] //

In[•]:= usEx61

Out[•]= {0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1}

In[•]:= BerlekampMasseyFull[usEx61] // TF

Out[•]//TableForm=
```

$\{2, 0, 1, 1\}$	$\{3, 3, 1, 1\}$
$\{2, 0, 1, 1\}$	$\{4, 3, 0, 1+z\}$
$\{2, 0, 1, 1\}$	$\{5, 3, 0, 1+z\}$
$\{2, 0, 1, 1\}$	$\{6, 3, 1, 1+z\}$
$\{6, 3, 1, 1+z\}$	$\{7, 4, 0, 1+z+z^4\}$
$\{6, 3, 1, 1+z\}$	$\{8, 4, 0, 1+z+z^4\}$
$\{6, 3, 1, 1+z\}$	$\{9, 4, 1, 1+z+z^4\}$
$\{9, 4, 1, 1+z+z^4\}$	$\{10, 6, 1, 1+z+z^3\}$
$\{9, 4, 1, 1+z+z^4\}$	$\{11, 6, 0, 1+z^2+z^3+z^5\}$
$\{9, 4, 1, 1+z+z^4\}$	$\{12, 6, 1, 1+z^2+z^3+z^5\}$
$\{12, 6, 1, 1+z^2+z^3+z^5\}$	$\{13, 7, 0, 1+z^2+z^4+z^5+z^7\}$
$\{12, 6, 1, 1+z^2+z^3+z^5\}$	$\{14, 7, 0, 1+z^2+z^4+z^5+z^7\}$
$\{12, 6, 1, 1+z^2+z^3+z^5\}$	$\{15, 7, 0, 1+z^2+z^4+z^5+z^7\}$

Example 6.1 [continued]

For instance, the first 10 terms $u_0 u_1 \ldots u_9$ are generated by the LFSR of width 6 with feedback polynomial $1 + z + z^3$; its taps are $\{1, 3\}$. Taking as the key $u_0 u_1 u_2 u_3 u_4 u_5 = 001111$, the first 30 terms of the keystream are:

$$\begin{aligned} k_i &= (0,0,1,1,1,1,0,1,0,0,1,1,1,0,1,0,0,1,1,1,\ldots) \\ u_i &= (0,0,1,1,1,1,0,1,0,0,0,0,0,0,1,0,1,0,0,1,\ldots) \\ &\quad\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \end{aligned}$$

Since $k_{10} \neq u_{10}$, running the Berlekamp–Massey algorithm on the first 11 bits $u_0 \ldots u_9 u_{10}$ gives a different LFSR. (The width stays as 6, but the taps change to $\{2, 3, 5\}$.) The new LFSR generates $u_0 \ldots u_9 u_{10} u_{11}$, so is also correct for the first 12 bits. This is why there is no change for $n = 12$.

For all $n \geq 13$ the output of the algorithm is the LFSR of width 7 and feedback polynomial $1 + z^2 + z^4 + z^5 + z^7$; as suggested on the problem sheet, this may also be found by the method of annihilators.

Preliminaries

Fix throughout a binary stream

$$u_0 u_1 u_2 \ldots.$$

Let $U_n(z) = u_0 + u_1 z + \cdots + u_{n-1} z^{n-1}$ be the polynomial recording the first n terms. Recall from §1 that the degree of a non-zero polynomial $h(z)$ is its highest power of z.

- Which of the following is a necessary and sufficient condition for an LFSR of width ℓ and taps T to be invertible?
  (A) $1 \in T$ (B) $1 \notin T$ (C) $\ell \in T$ (D) $\ell \notin T$
- The keystream 00010 01101 01111 is the output of the LFSR with taps $\{3, 4\}$ and what width(s)?
  (A) 4 (B) any $\ell \geq 4$ (C) any $\ell \geq 3$ (D) 4 or 5

Lemma 6.3

The word $u_0 u_1 \ldots u_{n-1}$ is the output of the LFSR with width ℓ and taps $T \subseteq \{1, \ldots, \ell\}$ if and only if $U_n(z) g_T(z) = h(z) + z^n r(z)$ for some polynomials $h(z)$ and $r(z)$ with $\deg h < \ell$.

Preliminaries

Fix throughout a binary stream

$$u_0 u_1 u_2 \ldots.$$

Let $U_n(z) = u_0 + u_1 z + \cdots + u_{n-1} z^{n-1}$ be the polynomial recording the first n terms. Recall from §1 that the degree of a non-zero polynomial $h(z)$ is its highest power of z.

- Which of the following is a necessary and sufficient condition for an LFSR of width ℓ and taps T to be invertible?
  (A) $1 \in T$ (B) $1 \notin T$ (C) $\ell \in T$ (D) $\ell \notin T$
- The keystream 00010 01101 01111 is the output of the LFSR with taps $\{3, 4\}$ and what width(s)?
  (A) 4 (B) any $\ell \geq 4$ (C) any $\ell \geq 3$ (D) 4 or 5

Lemma 6.3

The word $u_0 u_1 \ldots u_{n-1}$ is the output of the LFSR with width ℓ and taps $T \subseteq \{1, \ldots, \ell\}$ if and only if $U_n(z) g_T(z) = h(z) + z^n r(z)$ for some polynomials $h(z)$ and $r(z)$ with $\deg h < \ell$.

Preliminaries

Fix throughout a binary stream

$$u_0 u_1 u_2 \ldots.$$

Let $U_n(z) = u_0 + u_1 z + \cdots + u_{n-1} z^{n-1}$ be the polynomial recording the first n terms. Recall from §1 that the degree of a non-zero polynomial $h(z)$ is its highest power of z.

- Which of the following is a necessary and sufficient condition for an LFSR of width ℓ and taps T to be invertible?
  (A) $1 \in T$ (B) $1 \notin T$ (C) $\ell \in T$ (D) $\ell \notin T$
- The keystream 00010 01101 01111 is the output of the LFSR with taps $\{3, 4\}$ and what width(s)?
  (A) 4 (B) any $\ell \geq 4$ (C) any $\ell \geq 3$ (D) 4 or 5

Lemma 6.3

The word $u_0 u_1 \ldots u_{n-1}$ is the output of the LFSR with width ℓ and taps $T \subseteq \{1, \ldots, \ell\}$ if and only if $U_n(z) g_T(z) = h(z) + z^n r(z)$ for some polynomials $h(z)$ and $r(z)$ with $\deg h < \ell$.

Preliminaries

Fix throughout a binary stream

$$u_0 u_1 u_2 \ldots.$$

Let $U_n(z) = u_0 + u_1 z + \cdots + u_{n-1} z^{n-1}$ be the polynomial recording the first n terms. Recall from §1 that the degree of a non-zero polynomial $h(z)$ is its highest power of z.

- Which of the following is a necessary and sufficient condition for an LFSR of width ℓ and taps T to be invertible?
  (A) $1 \in T$ (B) $1 \notin T$ (C) $\ell \in T$ (D) $\ell \notin T$
- What is the minimum width and smallest set of taps of an LFSR generating 00010 00000 00000 ...?
  (A) $\ell = 0, T = \varnothing$ (B) $\ell = 3, T = \varnothing$ (C) $\ell = 4, T = \varnothing$ (D) $\ell = 4, T = \{4\}$

Lemma 6.3

The word $u_0 u_1 \ldots u_{n-1}$ is the output of the LFSR with width ℓ and taps $T \subseteq \{1, \ldots, \ell\}$ if and only if $U_n(z) g_T(z) = h(z) + z^n r(z)$ for some polynomials $h(z)$ and $r(z)$ with $\deg h < \ell$.

Preliminaries

Fix throughout a binary stream

$$u_0 u_1 u_2 \ldots.$$

Let $U_n(z) = u_0 + u_1 z + \cdots + u_{n-1} z^{n-1}$ be the polynomial recording the first n terms. Recall from §1 that the degree of a non-zero polynomial $h(z)$ is its highest power of z.

- Which of the following is a necessary and sufficient condition for an LFSR of width ℓ and taps T to be invertible?
  (A) $1 \in T$ (B) $1 \notin T$ (C) $\ell \in T$ (D) $\ell \notin T$
- What is the minimum width and smallest set of taps of an LFSR generating 00010 00000 00000 . . .?
  (A) $\ell = 0, T = \varnothing$ (B) $\ell = 3, T = \varnothing$ (C) $\ell = 4, T = \varnothing$ (D) $\ell = 4, T = \{4\}$

Lemma 6.3

The word $u_0 u_1 \ldots u_{n-1}$ is the output of the LFSR with width ℓ and taps $T \subseteq \{1, \ldots, \ell\}$ if and only if $U_n(z) g_T(z) = h(z) + z^n r(z)$ for some polynomials $h(z)$ and $r(z)$ with $\deg h < \ell$.

Example of Lemma 6.3

Example 6.4

Let $u = (0,0,1,1,1,1,0,1,0,0,0,0,0) = u_0 \dots u_{12}$ be the first 13 entries of the keystream in Example 6.1. The first 12 entries $u_0 \dots u_{11}$ are generated by the LFSR of width 6 with taps $\{2,3,5\}$. Correspondingly, by the 'if' direction of Lemma 6.3,

$$\begin{aligned}(z^2+z^3+z^4+z^5+z^7)g_{\{2,3,5\}}(z) &\\ &= (z^2+z^3+z^4+z^5+z^7)(1+z^2+z^3+z^5)\\ &= z^2+z^3+z^5+z^{12}\\ &= h(z)+z^{12}r(z)\end{aligned}$$

where $h(z) = z^2+z^3+z^5$ and $r(z) = 1$. This equation also shows that the 'only if' direction fails to hold when $n = 13$ since z^{12} is not of the form $z^{13}r(z)$. Correspondingly, by the 'only if' direction of Lemma 6.3, the LFSR generates $(0,0,1,1,1,1,0,1,0,0,0,0,1)$ rather than u.

At step n of the Berlekamp–Massey algorithm we have two LFSRs:

- An LFSR F_m of width ℓ_m with taps T_m, generating

$$u_0 u_1 \dots u_{m-1} \overline{u}_m \dots .$$

- An LFSR F_n of width ℓ_n with taps T_n, where $n > m$, generating

$$u_0 u_1 \dots u_{m-1} u_m \dots u_{n-1}.$$

Thus F_m is correct for the first m positions, and then wrong, since it generates $\overline{u}_m$ rather than u_m. If F_n generates $u_0 u_1 \dots u_{m-1} u_m \dots u_{n-1} u_n$ then case (a) applies and the algorithm returns F_n. The next proposition deals with case (b), when F_n outputs $\overline{u}_n$ rather than u_n.

Proposition 6.5

With the notation above, suppose that the LFSR F_n generates $u_0 u_1 \dots u_{n-1} \overline{u}_n$. The LFSR with feedback polynomial

$$z^{n-m} g_{T_m}(z) + g_{T_n}(z)$$

and width $\max(n - m + \ell_m, \ell_n)$ *generates* $u_0 u_1 \dots u_{n-1} u_n$.

Proof of Proposition 6.5

Proposition 6.5

With the notation above, suppose that the LFSR F_n generates $u_0 u_1 \dots u_{n-1} \overline{u}_n$. The LFSR with feedback polynomial

$$z^{n-m} g_{T_m}(z) + g_{T_n}(z)$$

and width $\max(n - m + \ell_m, \ell_n)$ *generates* $u_0 u_1 \dots u_{n-1} u_n$.

Notation: we write $[\geq a]$ to stand for a polynomial which is either 0, or whose *minimum* power of z is z^a or a higher power.

Consider the following statements

(A) $z^3 = [\geq 3]$

(B) $z^4 + z^5 + z^{20} = [\geq 3]$

(C) If $f(z) = [\geq 3]$ and $g(z) = [\geq 3]$ then $f(z) + g(z) = [\geq 3]$

(D) If $f(z) = [\geq 3]$ and $g(z) = [\geq 3]$ then $f(z) + g(z) \neq [\geq 4]$.

Which is the only false statement?

(A) (B) (C) (D)

Proof of Proposition 6.5

Proposition 6.5

With the notation above, suppose that the LFSR F_n generates $u_0 u_1 \dots u_{n-1} \overline{u}_n$. The LFSR with feedback polynomial

$$z^{n-m} g_{T_m}(z) + g_{T_n}(z)$$

and width $\max(n - m + \ell_m, \ell_n)$ *generates* $u_0 u_1 \dots u_{n-1} u_n$.

Notation: we write $[\geq a]$ to stand for a polynomial which is either 0, or whose *minimum* power of z is z^a or a higher power.

Consider the following statements

(A) $z^3 = [\geq 3]$

(B) $z^4 + z^5 + z^{20} = [\geq 3]$

(C) If $f(z) = [\geq 3]$ and $g(z) = [\geq 3]$ then $f(z) + g(z) = [\geq 3]$

(D) If $f(z) = [\geq 3]$ and $g(z) = [\geq 3]$ then $f(z) + g(z) \neq [\geq 4]$.

Which is the only false statement?

(A) (B) (C) (D)

Proof of Proposition 6.5

Proposition 6.5

With the notation above, suppose that the LFSR F_n generates $u_0 u_1 \dots u_{n-1} \overline{u}_n$. The LFSR with feedback polynomial

$$z^{n-m} g_{T_m}(z) + g_{T_n}(z)$$

and width $\max(n - m + \ell_m, \ell_n)$ *generates* $u_0 u_1 \dots u_{n-1} u_n$.

Lemma 6.3

The word $u_0 u_1 \dots u_{n-1}$ is the output of the LFSR with width ℓ and taps $T \subseteq \{1, \dots, \ell\}$ if and only if $U_n(z) g_{T_n}(z) = h(z) + z^n r(z)$ for some polynomials $h(z)$ and $r(z)$ with $\deg h < \ell$.

Notation reminder: We have already defined

$$U_r(z) = u_0 + u_1 z + \cdots + u_{r-1} z^{r-1}.$$

This takes r terms from the keystream, namely $u_0 u_1 \dots u_{r-1}$.

Example of Proposition 6.5

Example 6.6

Take the keystream $k_0 k_1 \ldots k_9$ of length 10 shown below:

$$\underset{0}{(}\underset{1}{1},\underset{2}{1},\underset{3}{1},\underset{4}{0},\underset{5}{1},\underset{6}{0},\underset{7}{1},\underset{8}{0},\underset{9}{0},\underset{}{0}).$$

The LFSR F_6 of width $\ell_6 = 3$ and taps $T_6 = \{1, 3\}$ generates the keystream

$$\underset{0}{(}\underset{1}{1},\underset{2}{1},\underset{3}{1},\underset{4}{0},\underset{5}{1},\underset{6}{0},\underset{7}{0},\underset{8}{1},\underset{9}{1},\underset{}{1}).$$

The LFSR F_7 of width $\ell_7 = 4$ and taps $T_7 = \{1, 4\}$ generates the keystream

$$\underset{0}{(}\underset{1}{1},\underset{2}{1},\underset{3}{1},\underset{4}{0},\underset{5}{1},\underset{6}{0},\underset{7}{1},\underset{8}{1},\underset{9}{0},\underset{}{0}).$$

Note that F_7 is wrong in position 7.

Example 6.6 [continued]

Using Proposition 6.5, taking $m = 6$ and $n = 7$ we compute

$$\begin{aligned} z^{n-m} g_{T_m} + g_{T_n}(z) &= z^{7-6} g_{\{1,3\}}(z) + g_{\{1,4\}}(z) \\ &= z(1 + z + z^3) + (1 + z + z^4) \\ &= 1 + z^2. \end{aligned}$$

This is the feedback polynomial of the LFSR F_8 with taps $T_8 = \{2\}$ and width $\ell_8 = n - m + \ell_m = 7 - 6 + 3 = 4$. As expected this generates

$$\begin{array}{cccccccccc} (1, & 1, & 1, & 0, & 1, & 0, & 1, & 0, & 1, & 0). \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array}$$

correct for the first 8 positions. (And then wrong for u_8.) Although the only tap in $\{2\}$ is 2, we still have to take the width of F_8 to be 4 (or more), to get the first 8 positions correct.

Continuing Example 6.6

Exercise 6.7

Continuing from the example, apply Proposition 6.5 taking $n = 8$, $m = 6$, and F_8 and F_6 as in Example 6.6. You should get the LFSR F_9 with taps $\{3, 5\}$ generating

$$\underset{0}{1}, \underset{1}{1}, \underset{2}{1}, \underset{3}{0}, \underset{4}{1}, \underset{5}{0}, \underset{6}{1}, \underset{7}{0}, \underset{8}{0}, \underset{9}{0}).$$

which is the full keystream. The width is now $8 - 6 + 3 = 5$; since 5 is a tap, this is the minimum possible width for these taps.

Continuing Example 6.6

Exercise 6.7

Continuing from the example, apply Proposition 6.5 taking $n = 8$, $m = 6$, and F_8 and F_6 as in Example 6.6. You should get the LFSR F_9 with taps $\{3, 5\}$ generating

$$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0).$$
$$0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

which is the full keystream. The width is now $8 - 6 + 3 = 5$; since 5 is a tap, this is the minimum possible width for these taps.

Further exercise: append a final bit $u_{10} = 1$ and update the LFSR in two different ways:

- Taking $m = 8$ using the LFSR of width 4 and taps $\{2\}$ wrong in position 8.
- Taking $m = 7$ using the LFSR of width 4 and taps $\{1, 4\}$ wrong in position 7.

Both give LFSRs generating 11101010001. Which has smaller width? (Click on for answer revealed above, see also Example 6.8.)

Continuing Example 6.6

Exercise 6.7

Continuing from the example, apply Proposition 6.5 taking $n = 8$, $m = 6$, and F_8 and F_6 as in Example 6.6. You should get the LFSR F_9 with taps $\{3, 5\}$ generating

$$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0).$$
$$0\ \ 1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7\ \ 8\ \ 9$$

which is the full keystream. The width is now $8 - 6 + 3 = 5$; since 5 is a tap, this is the minimum possible width for these taps.

Further exercise: append a final bit $u_{10} = 1$ and update the LFSR in two different ways:

- Taking $m = 8$ using the LFSR of width 4 and taps $\{2\}$ wrong in position 8. Taps $\{2, 3, 4, 5\}$, width $\max(10 - 8 + 4, 5) = 6$
- Taking $m = 7$ using the LFSR of width 4 and taps $\{1, 4\}$ wrong in position 7. Taps $\{4,5,7\}$, width $\max(10-7+4,5)=7$.

Both give LFSRs generating 11101010001. Which has smaller width? (Click on for answer revealed above, see also Example 6.8.)

Berlekamp–Massey algorithm

Let c be least such that $u_c \neq 0$. The algorithm defines LFSRs $F_c, F_{c+1}, \ldots$ so that each F_n has width ℓ_n and taps T_n and generates the first n positions of the keystream: $u_0, \ldots, u_{n-1}$.

- [Initialization] Set $T_c = \varnothing$, $\ell_c = 0$, $T_{c+1} = \varnothing$ and $\ell_{c+1} = c + 1$. Set $m = c$. Set $n = c + 1$.
- [Step] We have an LFSR F_n with taps T_n of width ℓ_n generating $u_0, \ldots, u_{n-1}$ and an LFSR F_m generating $u_0, \ldots, u_{m-1}, \overline{u}_m$.
  - (a) If F_n generates $u_0, \ldots, u_{n-1}, u_n$ then set $T_{n+1} = T_n$, $\ell_{n+1} = \ell_n$. This defines F_{n+1} with $F_{n+1} = F_n$. Keep m as it is.
  - (b) If F_n generates $u_0, \ldots, u_{n-1}, \overline{u}_n$, calculate

$$g(z) = z^{n-m} g_{T_m}(z) + g_{T_n}(z)$$

where, as usual, g_{T_m} and g_{T_n} are the feedback polynomials. Define T_{n+1} so that $g(z) = 1 + \sum_{t \in T_{n+1}} z^t$. Set

$$\ell_{n+1} = \max(\ell_n, n + 1 - \ell_n).$$

If $\ell_{n+1} > \ell_n$, update m to n, otherwise keep m as it is.

Thus m changes if and only if the width increases in step (b).

Example 6.8

We apply the Berlekamp–Massey algorithm to the keystream $(1,1,1,0,1,0,1,0,0,0,1)$ from Example 6.6 extended by one extra bit $u_{10} = 1$. After initialization we have $T_0 = \varnothing$, $\ell_0 = 0$, $T_1 = \varnothing$, $\ell_1 = 1$. Case (a) applies in each step n for $n \in \{2,4,5,9\}$. The table below shows the steps when case (b) applies.

n	T_n	ℓ_n	m	T_m	$n-m$	T_{n+1}	ℓ_{n+1}
1	$\varnothing$	1	0	$\varnothing$	1	$\{1\}$	1
3	$\{1\}$	1	0	$\varnothing$	3	$\{1,3\}$	3
6	$\{1,3\}$	3	3	$\{1\}$	3	$\{1,4\}$	4
7	$\{1,4\}$	4	6	$\{1,3\}$	1	$\{2\}$	4
8	$\{2\}$	4	6	$\{1,3\}$	2	$\{3,5\}$	5
10	$\{3,5\}$	5	8	$\{2\}$	2	$\{2,3,4,5\}$	6

Exercise on Example 6.8

Exercise 6.9

- Run the algorithm starting with step 1, in which you should define $T_2 = \{1\}$, and finishing with step 6, in which you should define $T_7 = \{1, 4\}$.
- Then check that steps 7 and 8 of the algorithm are exactly what we did in Example 6.6 and Exercise 6.7.
- At step 9 you should find that case (a) applies; check that step 10 finishes with the LFSR F_{11} of width $\ell_{11} = 6$ and taps $T_{11} = \{2, 3, 4, 5\}$, generating $u_0 u_1 \ldots u_{10}$.

Berlekamp–Massey theorem

To prove that the LFSRs defined by running the Berlekamp–Massey algorithm have minimal possible width we need the following lemma. The proof is not obvious, but if you think 'what can I possibly do using Lemma 6.3' you should find the main idea.

Lemma 6.10

Let $n \geq \ell$. If an LFSR F of width ℓ generates the keystream $(u_0, u_1, \ldots, u_{n-1}, b)$ of length $n+1$ then any LFSR F' generating the keystream $(u_0, u_1, \ldots, u_{n-1}, \overline{b})$ has width ℓ' where $\ell' \geq n + 1 - \ell$.

Quiz: The keystream $u_0 u_1 u_2 \ldots = 000100110101111$ is a generating cycle of the LFSR of width 4 with taps $\{3, 4\}$. Suppose we flip bit u_9 to get 000100110001111. What is a lower bound on the width of an LFSR generating $u_0 u_1 u_2 \ldots \overline{u}_9$?

(A) 5 (B) 6 (C) 7 (D) 10

Berlekamp–Massey theorem

To prove that the LFSRs defined by running the Berlekamp–Massey algorithm have minimal possible width we need the following lemma. The proof is not obvious, but if you think 'what can I possibly do using Lemma 6.3' you should find the main idea.

Lemma 6.10

Let $n \geq \ell$. If an LFSR F of width ℓ generates the keystream $(u_0, u_1, \ldots, u_{n-1}, b)$ of length $n+1$ then any LFSR F' generating the keystream $(u_0, u_1, \ldots, u_{n-1}, \overline{b})$ has width ℓ' where $\ell' \geq n + 1 - \ell$.

Quiz: The keystream $u_0 u_1 u_2 \ldots = 000100110101111$ is a generating cycle of the LFSR of width 4 with taps $\{3, 4\}$. Suppose we flip bit u_9 to get 000100110001111. What is a lower bound on the width of an LFSR generating $u_0 u_1 u_2 \ldots \overline{u}_9$?

(A) 5 (B) 6 (C) 7 (D) 10

Berlekamp–Massey theorem

To prove that the LFSRs defined by running the Berlekamp–Massey algorithm have minimal possible width we need the following lemma. The proof is not obvious, but if you think 'what can I possibly do using Lemma 6.3' you should find the main idea.

Lemma 6.10

Let $n \geq \ell$. If an LFSR F of width ℓ generates the keystream $(u_0, u_1, \ldots, u_{n-1}, b)$ of length $n+1$ then any LFSR F' generating the keystream $(u_0, u_1, \ldots, u_{n-1}, \overline{b})$ has width ℓ' where $\ell' \geq n + 1 - \ell$.

```
In[•]:= Keystream[{3, 4}, {0, 0, 0, 1}]

Out[•]= {0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1}

In[•]:= BerlekampMasseyFull[{0, 0, 0, 1, 0, 0, 1, 1, 0, 0}] // TF

Out[•]//TableForm=
{3, 0, 1, 1}                    {4, 4, 0, 1}
{3, 0, 1, 1}                    {5, 4, 0, 1}
{3, 0, 1, 1}                    {6, 4, 1, 1}
{3, 0, 1, 1}                    {7, 4, 1, 1 + z^3}
{3, 0, 1, 1}                    {8, 4, 0, 1 + z^3 + z^4}
{3, 0, 1, 1}                    {9, 4, 1, 1 + z^3 + z^4}
{9, 4, 1, 1 + z^3 + z^4}        {10, 6, 0, 1 + z^3 + z^4 + z^6}

In[•]:= Keystream[{3, 4, 6}, {0, 0, 0, 1, 0, 0}, 15]

Out[•]= {0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1}
```

Berlekamp–Massey theorem

To prove that the LFSRs defined by running the Berlekamp–Massey algorithm have minimal possible width we need the following lemma. The proof is not obvious, but if you think 'what can I possibly do using Lemma 6.3' you should find the main idea.

Lemma 6.10

Let $n \geq \ell$. If an LFSR F of width ℓ generates the keystream $(u_0, u_1, \ldots, u_{n-1}, b)$ of length $n+1$ then any LFSR F' generating the keystream $(u_0, u_1, \ldots, u_{n-1}, \overline{b})$ has width ℓ' where $\ell' \geq n + 1 - \ell$.

Lemma 6.3

The word $u_0 u_1 \ldots u_{n-1}$ is the output of the LFSR with width ℓ and taps $T \subseteq \{1, \ldots, \ell\}$ if and only if $U_n(z) g_T(z) = h(z) + z^n r(z)$ for some polynomials $h(z)$ and $r(z)$ with $\deg h < \ell$.

I got lost at the end of the proof by thinking that $g_T(z)$ somehow had to have degree $< \ell$. This is wrong: the degree can be ℓ, and correspondingly ℓ can be a tap. There is a video on Moodle and a scan of a correct proof (you just need to amend the end).

Berlekamp–Massey theorem

To prove that the LFSRs defined by running the Berlekamp–Massey algorithm have minimal possible width we need the following lemma. The proof is not obvious, but if you think 'what can I possibly do using Lemma 6.3' you should find the main idea.

Lemma 6.10

Let $n \geq \ell$. If an LFSR F of width ℓ generates the keystream $(u_0, u_1, \ldots, u_{n-1}, b)$ of length $n+1$ then any LFSR F' generating the keystream $(u_0, u_1, \ldots, u_{n-1}, \overline{b})$ has width ℓ' where $\ell' \geq n + 1 - \ell$.

Recall that step n of the Berlekamp–Massey algorithm returns an LFSR F_{n+1} with taps T_{n+1} and width ℓ_{n+1} generating $u_0 \ldots u_{n-1} u_n$.

Theorem 6.11

With the notation above, $\max T_{n+1} \leq \ell_{n+1}$. *Moreover ℓ_{n+1} is the least width of any LFSR generating $u_0, \ldots, u_{n-1}, u_n$.*

Example of Lemma 6.10 and Linear Complexity

The *linear complexity* of a word $u_0 u_1 \ldots u_{n-1}$ is the minimal width of an LFSR that generates it. By Lemma 6.10 a good way to get a word of high linear complexity is to take the output of a small width LFSR and then flip the last bit.

```
In[•]:= ks := Keystream[{2, 5}, {0, 0, 0, 0, 1}, 20]; ks

Out[•]= {0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1}

In[•]:= ksP = ks; ksP[[20]] = 0; ksP

Out[•]= {0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0}

In[•]:= BerlekampMassey[ks]

Out[•]= {20, 5, 0, 1 + z^2 + z^5}

In[•]:= BerlekampMasseyFull[ksP][[-2 ;; -1]] // TF

Out[•]//TableForm=
{4, 0, 1, 1}                    {19, 5, 1, 1 + z^2 + z^5}
{19, 5, 1, 1 + z^2 + z^5}       {20, 15, 0, 1 + z^2 + z^5 + z^15}
```

Berlekamp–Massey for Integer Sequences

The Berlekamp–Massey algorithm generalizes to arbitrary fields, including the field of rational numbers: see `LFSRs.nb`.

Small example: twice Fibonacci sequence: try changing an early term, or the characteristic (change final argument from 0 to an odd prime)

```
In[•]:= fs := {0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144}; ksTest := 2 * fs; ksTest
Out[•]= {0, 2, 2, 4, 6, 10, 16, 26, 42, 68, 110, 178, 288}

In[•]:= BerlekampMasseyFull[ksTest, 0][[1 ;; 6]] // TF
Out[•]//TableForm=
{1, 0, 2, 1}    {2, 2, 2, 1}
{1, 0, 2, 1}    {3, 2, 2, 1 - z}
{1, 0, 2, 1}    {4, 2, 0, 1 - z - z^2}
{1, 0, 2, 1}    {5, 2, 0, 1 - z - z^2}
{1, 0, 2, 1}    {6, 2, 0, 1 - z - z^2}
{1, 0, 2, 1}    {7, 2, 0, 1 - z - z^2}
```

Example: number of regions made by joining up all pairs of n points around the circle

```
In[•]:= BerlekampMassey[{1, 2, 4, 8, 16, 31, 57, 99, 163, 256, 386}, 0]
Out[•]= {11, 5, 0, 1 - 5 z + 10 z^2 - 10 z^3 + 5 z^4 - z^5}

In[•]:= Keystream[{5, -10, 10, -5, 1}, {1, 2, 4, 8, 16, 31}, 15, 0]
Out[•]= {1, 2, 4, 8, 16, 31, 57, 99, 163, 256, 386, 562, 794, 1093, 1471}
```

Berlekamp–Massey for Integer Sequences

The Berlekamp–Massey algorithm generalizes to arbitrary fields, including the field of rational numbers: see `LFSRs.nb`.

Smaller example: triangular numbers starting 1, 3, 6, ...

```
In[•]:= BerlekampMassey[{1, 3, 6, 10, 15, 21, 28, 36}, 0]
```

$$\text{Out}[\bullet]= \left\{8,\ 3,\ 0,\ 1 - 3\,z + 3\,z^2 - z^3\right\}$$

```
In[•]:= (1 - z) ^ 3 * (1 + 3 z + 6 z ^ 2 + 10 z ^ 3 + 15 z ^ 4 + 21 z ^ 5 + 28 z ^ 6 + 36 z ^ 7) // Expa
```

$$\text{Out}[\bullet]= 1 - 45\,z^8 + 80\,z^9 - 36\,z^{10}$$

Linear Complexity

Recall that the *linear complexity* of a word $u_0 u_1 \dots u_{n-1}$ is the minimal width of an LFSR that generates it. Modern stream ciphers aim to generate keystreams with high linear complexity. Take the m-quadratic stream cipher from Example 8.5. If $m = 1$ the keystream $u_0 u_1 \dots u_{29}$ for $k = 10101$ and $k' = 101010$ is

$$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1).$$

The table below shows the linear complexity of the first n bits of the keystream for small n and m.

$m \backslash n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	1	2	2	2	2	5	5	5	5	5	5	5	5	5
2	0	2	2	2	2	2	5	5	5	5	5	5	5	5	5
3	0	0	0	4	4	4	4	4	4	6	6	6	6	6	6
4	0	0	0	0	0	7	7	7	7	7	7	7	7	7	8
5	0	0	0	0	5	5	5	5	5	5	5	7	7	7	8

For $n = 5$ the linear complexity is about $n/2$: this is the expected linear complexity of a random sequence of bits.

§7 Linear cryptanalysis

Example 7.1

Let $S : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ be the S-box in the Q-block cipher (see Example 9.5 in the main notes), defined by

$$S\big((x_0, x_1, x_2, x_3)\big) = (x_2, x_3, x_0 + x_1x_2, x_1 + x_2x_3).$$

(a) Suppose we look at position 0 of the output by considering $L_{\{0\}} \circ S : \mathbb{F}_2^4 \to \mathbb{F}_2$. We have

$$\begin{aligned}(L_{\{0\}} \circ S)\big((x_0, x_1, x_2, x_3)\big) &= L_{\{0\}}(x_2, x_3, x_0 + x_1x_2, x_1 + x_2x_3) \\ &= x_2 \\ &= L_{\{2\}}\big((x_0, x_1, x_2, x_3)\big).\end{aligned}$$

Hence $L_{\{0\}} \circ S = L_{\{2\}}$. By Lemma 4.4,

$$\operatorname{corr}(L_{\{0\}} \circ S, L_T) = \begin{cases} 1 & \text{if } T = \{2\} \\ 0 & \text{otherwise.} \end{cases}$$

Example 6.1 [continued]

(b) Instead if we look at position 2, the relevant boolean function is $L_{\{2\}} \circ S$, for which $L_{\{2\}} \circ S\big((x_0, x_1, x_2, x_3)\big) = x_0 + x_1 x_2$. *Exercise:* show that

$$\mathrm{corr}(L_{\{2\}} \circ S, L_T) = \begin{cases} \frac{1}{2} & \text{if } T = \{0\}, \{0,1\}, \{0,2\} \\ -\frac{1}{2} & \text{if } T = \{0,1,2\} \\ 0 & \text{otherwise} \end{cases} .$$

Example 7.2

For $k \in \mathbb{F}_2^{12}$ let $e_k : \mathbb{F}_2^8 \to \mathbb{F}_2^8$ be the Q-block cipher, as defined in Example 8.4. Then $e_k\big((v,w)\big) = (v',w')$ where

$$v' = w + S\big(v + S(w + k^{(1)}) + k^{(2)}\big).$$

Recall that $k^{(1)} = (k_0, k_1, k_2, k_3)$ and $k^{(2)} = (k_4, k_5, k_6, k_7)$. Example 7.1 suggests considering $\mathrm{corr}(L_{\{0\}} \circ e_k, L_{\{2\}})$. We have

$$(L_{\{0\}} \circ e_k)\big((v,w)\big) = L_{\{0\}}\big((v',w')\big) = v'_0$$
$$L_{\{2\}}\big((v,w)\big) = v_2.$$

Exercise: using that $k_0^{(1)} = k_0$, $k_1^{(1)} = k_1$, $k_2^{(1)} = k_2$ and $k_2^{(2)} = k_6$, check that

$$v'_0 = v_2 + (w_1 + k_1)(w_2 + k_2) + k_0 + k_6.$$

Example 7.2 [continued]

By definition

$$\begin{aligned}\mathrm{corr}(L_{\{0\}} \circ e_k, L_{\{2\}}) &= \frac{1}{2^8} \sum_{(v,w)\in\mathbb{F}_2^8} (-1)^{v_2+(w_1+k_1)(w_2+k_2)+k_0+k_6}(-1)^{v_2} \\ &= \frac{1}{2^8}(-1)^{k_0+k_6} \sum_{(v,w)\in\mathbb{F}_2^8} (-1)^{(w_1+k_1)(w_2+k_2)} \\ &= (-1)^{k_0+k_6}\frac{1}{2^2} \sum_{w_1,w_2\in\mathbb{F}_2} (-1)^{(w_1+k_1)(w_2+k_2)}\end{aligned}$$

where the third line follows because the summand for (v, w) is the same for all 2^6 pairs with the same w_1 and w_2. In $\sum_{w_1,w_2\in\mathbb{F}_2}(-1)^{(w_1+k_1)(w_2+k_2)}$, the values of k_1 and k_2 are irrelevant.

Example 7.2 [continued]

By definition

$$\begin{aligned}\operatorname{corr}(L_{\{0\}} \circ e_k, L_{\{2\}}) &= \frac{1}{2^8} \sum_{(v,w)\in\mathbb{F}_2^8} (-1)^{v_2+(w_1+k_1)(w_2+k_2)+k_0+k_6}(-1)^{v_2} \\ &= \frac{1}{2^8}(-1)^{k_0+k_6} \sum_{(v,w)\in\mathbb{F}_2^8} (-1)^{(w_1+k_1)(w_2+k_2)} \\ &= (-1)^{k_0+k_6}\frac{1}{2^2} \sum_{w_1,w_2\in\mathbb{F}_2} (-1)^{(w_1+k_1)(w_2+k_2)}\end{aligned}$$

where the third line follows because the summand for (v, w) is the same for all 2^6 pairs with the same w_1 and w_2. In $\sum_{w_1,w_2\in\mathbb{F}_2}(-1)^{(w_1+k_1)(w_2+k_2)}$, the values of k_1 and k_2 are irrelevant. For instance, if both are 0 we average $(-1)^{w_1 w_2}$ over all four $(w_1, w_2) \in \mathbb{F}_2^2$ to get $\frac{1}{2}$; if both are 1 we average $(-1)^{(w_1+1)(w_2+1)}$, seeing the same summands in a different order, and still getting $\frac{1}{2}$. Hence $\frac{1}{2^2}\sum_{w_1,w_2\in\mathbb{F}_2}(-1)^{(w_1+k_1)(w_2+k_2)} = \frac{1}{2}$ and

$$\operatorname{corr}(L_{\{0\}} \circ e_k, L_{\{2\}}) = \tfrac{1}{2}(-1)^{k_0+k_6}$$

Attack on the Q-block cipher

We can estimate this correlation from a collection of plaintext/ciphertext pairs $(v, w), (v', w')$ by computing $(-1)^{v'_0+v_2}$ for each pair. The mean should be close to $\frac{1}{2}(-1)^{k_0+k_6}$, and the sign then tells us $k_0 + k_6$. There are similar high correlations of $\frac{1}{2}$ for output bit 1, and one can usefully 'tap' with $\{2, 5\}$ and $\{2, 6\}$ as well as $\{2\}$ on the input side. Using these one learns k_1, k_2 and k_3 as well as $k_1 + k_7$. (See Question 7 on Problem Sheet 8.)

Exercise 7.3

Given $k_0 + k_6, k_1 + k_7, k_1, k_2, k_3$, how many possibilities are there for the key in the Q-block cipher?

Attack on the Q-block cipher

We can estimate this correlation from a collection of plaintext/ciphertext pairs $(v, w), (v', w')$ by computing $(-1)^{v'_0+v_2}$ for each pair. The mean should be close to $\frac{1}{2}(-1)^{k_0+k_6}$, and the sign then tells us $k_0 + k_6$. There are similar high correlations of $\frac{1}{2}$ for output bit 1, and one can usefully 'tap' with $\{2, 5\}$ and $\{2, 6\}$ as well as $\{2\}$ on the input side. Using these one learns k_1, k_2 and k_3 as well as $k_1 + k_7$. (See Question 7 on Problem Sheet 8.)

Exercise 7.3

Given $k_0 + k_6, k_1 + k_7, k_1, k_2, k_3$, how many possibilities are there for the key in the Q-block cipher?

The attack by differential cryptanalysis required chosen plaintexts. The attack by linear cryptanalysis works with any observed collection of plaintext/ciphertext pairs. It is therefore more widely applicable, as well as more powerful.

How to Find High Correlations

In the attack on the Q-Block Cipher we saw that the correlation depended on the key only by a sign. This is because key addition, as is almost universally the case for block ciphers, was done in $\mathbb{F}_2^n$.

Lemma 7.4

Fix $k \in \mathbb{F}_2^n$. Define $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ by $F(x) = x + k$. Then

$$\text{corr}(L_T \circ F, L_U) = \begin{cases} (-1)^{L_T(k)} & \text{if } T = U \\ 0 & \text{if } T \neq U. \end{cases}$$

How to Find High Correlations

In the attack on the Q-Block Cipher we saw that the correlation depended on the key only by a sign. This is because key addition, as is almost universally the case for block ciphers, was done in $\mathbb{F}_2^n$.

Lemma 7.4

Fix $k \in \mathbb{F}_2^n$. Define $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ by $F(x) = x + k$. Then

$$\operatorname{corr}(L_T \circ F, L_U) = \begin{cases} (-1)^{L_T(k)} & \text{if } T = U \\ 0 & \text{if } T \neq U. \end{cases}$$

Another very useful result gives correlations through the composition of two functions. The 'output' side has to be on the left, in order to agree with matrix multiplication.

Proposition 7.5

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be functions. For $S, T \subseteq \{0, 1, \ldots, n-1\}$,

$$\operatorname{corr}(L_S \circ G \circ F, L_T) = \sum_{U \subseteq \{0,1,\ldots,n-1\}} \operatorname{corr}(L_S \circ G, L_U) \operatorname{corr}(L_U \circ F, L_T).$$

Example 7.6

(1) Take $G(x_0, x_1) = (x_0, x_0x_1)$. The matrix of correlations, with rows (output taps) and columns (input taps) labelled $\varnothing$, $\{0\}$, $\{1\}$, $\{0,1\}$ is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

(2) By Lemma 7.4, the matrix for $(x_0, x_1) \mapsto (x_0 + 1, x_1)$ is diagonal, with entries $1, -1, 1, 1$.

(3) Hence $H(x_0, x_1) = (x_0 + 1, x_0x_1 + x_1) = (\overline{x}_0, \overline{x}_0x_1)$ has correlation matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

Application of Proposition 7.5 to Q-block cipher

Let $F : \mathbb{F}_2^3 \to \mathbb{F}_2^3$ be the S-box in the 3 bit version of the Q-block cipher, so $F\big((x_0, x_1, x_2)\big) = (x_1, x_2, x_0 + x_1x_2)$. The matrix below shows the correlations,

$$\begin{pmatrix}
1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\
\cdot & \frac{1}{2} & \cdot & \frac{1}{2} & \cdot & \frac{1}{2} & \cdot & -\frac{1}{2} \\
\cdot & \frac{1}{2} & \cdot & \frac{1}{2} & \cdot & -\frac{1}{2} & \cdot & \frac{1}{2} \\
\cdot & \frac{1}{2} & \cdot & -\frac{1}{2} & \cdot & \frac{1}{2} & \cdot & \frac{1}{2} \\
\cdot & -\frac{1}{2} & \cdot & \frac{1}{2} & \cdot & \frac{1}{2} & \cdot & \frac{1}{2}
\end{pmatrix}$$

using $\cdot$ for a 0 correlation, with subsets ordered

$$\varnothing, \{0\}, \{1\}, \{0,1\}, \{2\}, \{0,2\}, \{1,2\}, \{0,1,2\}.$$

For example the first four rows show that tapping the output in positions $\varnothing$, $\{0\}$, $\{1\}$, or $\{0,1\}$ gives a linear function.

Application of Proposition 7.5 to Q-block cipher

Let $F : \mathbb{F}_2^3 \to \mathbb{F}_2^3$ be the S-box in the 3 bit version of the Q-block cipher, so $F\big((x_0, x_1, x_2)\big) = (x_1, x_2, x_0 + x_1x_2)$. The matrix below shows the correlations,

$$\begin{pmatrix}
1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\
\cdot & \frac{1}{2} & \cdot & \frac{1}{2} & \cdot & \frac{1}{2} & \cdot & -\frac{1}{2} \\
\cdot & \frac{1}{2} & \cdot & \frac{1}{2} & \cdot & -\frac{1}{2} & \cdot & \frac{1}{2} \\
\cdot & \frac{1}{2} & \cdot & -\frac{1}{2} & \cdot & \frac{1}{2} & \cdot & \frac{1}{2} \\
\cdot & -\frac{1}{2} & \cdot & \frac{1}{2} & \cdot & \frac{1}{2} & \cdot & \frac{1}{2}
\end{pmatrix}$$

using $\cdot$ for a 0 correlation, with subsets ordered

$$\varnothing, \{0\}, \{1\}, \{0,1\}, \{2\}, \{0,2\}, \{1,2\}, \{0,1,2\}.$$

By taking powers of this matrix we can compute correlations through any power of F.