Boolean Functions in Cryptology - Introduction

Petr Veselý

7. dubna 2010

Outline

Outline

Outline

Outline

What is a boolean function?

What is a boolean function?

- Informally: it is a mapping $\mathbb{Z}_2^n \to \mathbb{Z}_2^m$
- Formally: later

What is a boolean function?

- Informally: it is a mapping $\mathbb{Z}_2^n \to \mathbb{Z}_2^m$
- Formally: later

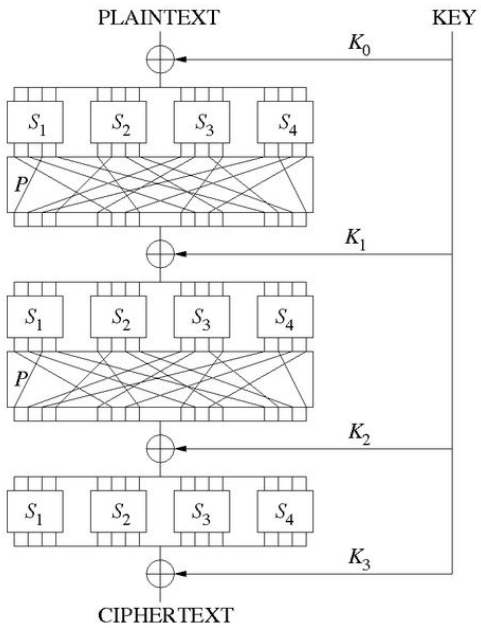
What is a cipher?

- Informally: a way to make a message unreadable for everyone except those who have a secret key
- Formally: a cipher system consists of
  a finite space P of all plaintexts,
  a finite space C of al ciphertexts,
  a finite space K of al keys,
  a set E of mappings $e_k : P \to C, k \in K$ and
  a set D of mappings $d_k : C \to P, k \in K$
  such that $d_k(e_k(p)) = p$ for all $p \in P$, $k \in K$

What is a cipher?

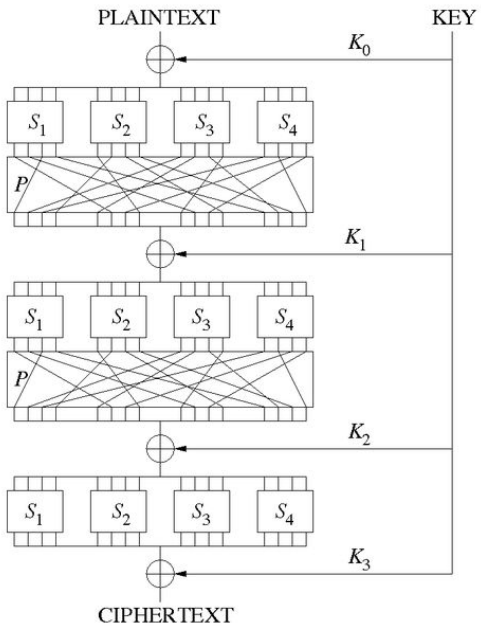
- Informally: a way to make a message unreadable for everyone except those who have a secret key
- Formally: a cipher system consists of
  a finite space P of all plaintexts,
  a finite space C of al ciphertexts,
  a finite space K of al keys,
  a set E of mappings $e_k : P \to C, k \in K$ and
  a set D of mappings $d_k : C \to P, k \in K$
  such that $d_k(e_k(p)) = p$ for all $p \in P$, $k \in K$

Building blocks of a (block) cipher



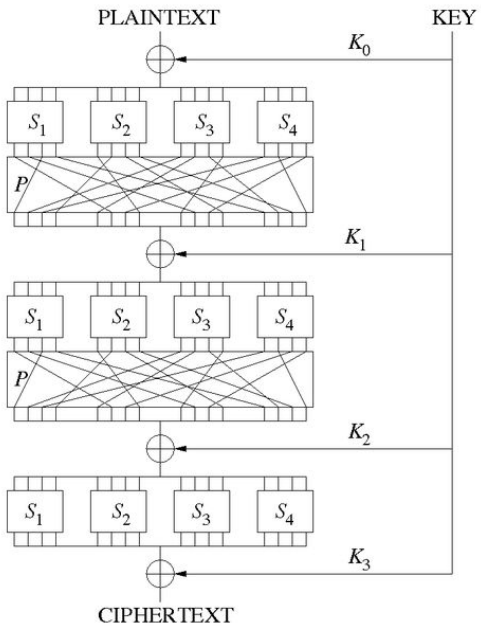
- Permutations
- Substitutions (S-Boxes)
- block ciphers are (built of) boolean functions

Building blocks of a (block) cipher



- Permutations
- Substitutions (S-Boxes)
- block ciphers are (built of) boolean functions

Building blocks of a (block) cipher



- Permutations
- Substitutions (S-Boxes)
- block ciphers are (built of) boolean functions

S-Boxes

S_5		Middle 4 bits of input															
		0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
Outer bits	**00**	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

it is a good idea to use nonlinear S-Boxes (as will Michal explain)

What are boolean functions

- boolean function is a mapping $\mathbb{Z}_2^n \to \mathbb{Z}_2^m$
- binary boolean function is a mapping $h : \mathbb{Z}_2^n \to \mathbb{Z}_2$
- boolean function $f(a) : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ can be expressed as $(f_1(a), \ldots f_m(a)), f_i : \mathbb{Z}_2^n \to \mathbb{Z}_2$

What are boolean functions

- boolean function is a mapping $\mathbb{Z}_2^n \to \mathbb{Z}_2^m$
- binary boolean function is a mapping $h : \mathbb{Z}_2^n \to \mathbb{Z}_2$
- boolean function $f(a) : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ can be expressed as $(f_1(a), \ldots f_m(a)), f_i : \mathbb{Z}_2^n \to \mathbb{Z}_2$

What are boolean functions

- boolean function is a mapping $\mathbb{Z}_2^n \to \mathbb{Z}_2^m$
- binary boolean function is a mapping $h : \mathbb{Z}_2^n \to \mathbb{Z}_2$
- boolean function $f(a) : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ can be expressed as $(f_1(a), ...f_m(a)), f_i : \mathbb{Z}_2^n \to \mathbb{Z}_2$

Different representations of binary boolean functions

- table of values
- logical formulas
- algebraic normal form
  $f(a) = s_0 \oplus \bigoplus s_i a_i \oplus \bigoplus s_{ij} a_i a_j \oplus \ldots \oplus s_{1,2,..,n} a_1 a_2 \ldots a_n$

Different representations of binary boolean functions

- table of values
- logical formulas
- algebraic normal form

$$f(a) = s_0 \oplus \bigoplus s_i a_i \oplus \bigoplus s_{ij} a_i a_j \oplus \ldots \oplus s_{1,2,..,n} a_1 a_2 \ldots a_n$$

Different representations of binary boolean functions

- table of values
- logical formulas
- algebraic normal form
  $f(a) = s_0 \oplus \bigoplus s_i a_i \oplus \bigoplus s_{ij} a_i a_j \oplus \ldots \oplus s_{1,2,..,n} a_1 a_2 \ldots a_n$

Various definitions

- **Def.: Parity function (parity) is a linear binary boolean function**
- parity f on $\mathbb{Z}_2^n$ can be uniquely expressed as a vector $u \in \mathbb{Z}_2^n$, such that $f(a) = u^T a$
- there are 2^n parity functions on $\mathbb{Z}_2^n$
- parity functions are always balanced (except for the trivial one)
- **Def.: Distance of binary boolean functions $d(f, g)$ is the number of inputs $a \in \mathbb{Z}_2^n$ s.t. $f(a) \neq g(a)$**
- $d(f, g) = \sum f(u) \oplus g(u)$

Various definitions

- **Def.: Parity function (parity) is a linear binary boolean function**
- parity f on $\mathbb{Z}_2^n$ can be uniquely expressed as a vector $u \in \mathbb{Z}_2^n$, such that $f(a) = u^T a$
- there are 2^n parity functions on $\mathbb{Z}_2^n$
- parity functions are always balanced (except for the trivial one)
- **Def.: Distance of binary boolean functions $d(f, g)$ is the number of inputs $a \in \mathbb{Z}_2^n$ s.t. $f(a) \neq g(a)$**
- $d(f, g) = \sum f(u) \oplus g(u)$

Various definitions

- **Def.: Parity function (parity) is a linear binary boolean function**
- parity f on $\mathbb{Z}_2^n$ can be uniquely expressed as a vector $u \in \mathbb{Z}_2^n$, such that $f(a) = u^T a$
- there are 2^n parity functions on $\mathbb{Z}_2^n$
- parity functions are always balanced (except for the trivial one)
- **Def.: Distance of binary boolean functions $d(f, g)$ is the number of inputs $a \in \mathbb{Z}_2^n$ s.t. $f(a) \neq g(a)$**
- $d(f, g) = \sum f(u) \oplus g(u)$

Various definitions

- **Def.: Parity function (parity) is a linear binary boolean function**
- parity f on $\mathbb{Z}_2^n$ can be uniquely expressed as a vector $u \in \mathbb{Z}_2^n$, such that $f(a) = u^T a$
- there are 2^n parity functions on $\mathbb{Z}_2^n$
- parity functions are always balanced (except for the trivial one)
- **Def.: Distance of binary boolean functions $d(f, g)$ is the number of inputs $a \in \mathbb{Z}_2^n$ s.t. $f(a) \neq g(a)$**
- $d(f, g) = \sum f(u) \oplus g(u)$

Various definitions

- **Def.: Parity function (parity) is a linear binary boolean function**
- parity f on $\mathbb{Z}_2^n$ can be uniquely expressed as a vector $u \in \mathbb{Z}_2^n$, such that $f(a) = u^T a$
- there are 2^n parity functions on $\mathbb{Z}_2^n$
- parity functions are always balanced (except for the trivial one)
- **Def.: Distance of binary boolean functions $d(f, g)$ is the number of inputs $a \in \mathbb{Z}_2^n$ s.t. $f(a) \neq g(a)$**
- $d(f, g) = \sum f(u) \oplus g(u)$

Various definitions

- **Def.: Parity function (parity) is a linear binary boolean function**
- parity f on $\mathbb{Z}_2^n$ can be uniquely expressed as a vector $u \in \mathbb{Z}_2^n$, such that $f(a) = u^T a$
- there are 2^n parity functions on $\mathbb{Z}_2^n$
- parity functions are always balanced (except for the trivial one)
- **Def.: Distance of binary boolean functions $d(f, g)$ is the number of inputs $a \in \mathbb{Z}_2^n$ s.t. $f(a) \neq g(a)$**
- $d(f, g) = \sum f(u) \oplus g(u)$

Various definitions (cont.)

- **Def.: Real-valued counterpart of a binary boolean function f is defined as $\widehat{f}(u) = (-1)^{f(u)}$**
- $\widehat{f(a) \oplus g(a)} = \widehat{f}(a)\widehat{g}(a)$
- **Def.: Inner product** $< \widehat{f}, \widehat{g} >= \sum \widehat{f}(a)\widehat{g}(a)$
- this inner product defines a norm $\|\widehat{f}\| = \sqrt{< \widehat{f}, \widehat{f} >}$
- for a binary boolean function from $\mathbb{Z}_2^n$ this norm is always $2^{n/2}$

Various definitions (cont.)

- **Def.: Real-valued counterpart of a binary boolean function f is defined as $\widehat{f}(u) = (-1)^{f(u)}$**
- $\widehat{f(a) \oplus g(a)} = \widehat{f}(a)\widehat{g}(a)$
- **Def.: Inner product** $< \widehat{f}, \widehat{g} >= \sum \widehat{f}(a)\widehat{g}(a)$
- this inner product defines a norm $\|\widehat{f}\| = \sqrt{< \widehat{f}, \widehat{f} >}$
- for a binary boolean function from $\mathbb{Z}_2^n$ this norm is always $2^{n/2}$

Various definitions (cont.)

- **Def.: Real-valued counterpart of a binary boolean function f is defined as $\widehat{f}(u) = (-1)^{f(u)}$**
- $\widehat{f(a) \oplus g(a)} = \widehat{f}(a)\widehat{g}(a)$
- **Def.: Inner product $< \widehat{f}, \widehat{g} >= \sum \widehat{f}(a)\widehat{g}(a)$**
- this inner product defines a norm $\|\widehat{f}\| = \sqrt{< \widehat{f}, \widehat{f} >}$
- for a binary boolean function from $\mathbb{Z}_2^n$ this norm is always $2^{n/2}$

Various definitions (cont.)

- **Def.: Real-valued counterpart of a binary boolean function f is defined as $\widehat{f}(u) = (-1)^{f(u)}$**
- $\widehat{f(a) \oplus g(a)} = \widehat{f}(a)\widehat{g}(a)$
- **Def.: Inner product** $< \widehat{f}, \widehat{g} >= \sum \widehat{f}(a)\widehat{g}(a)$
- this inner product defines a norm $\|\widehat{f}\| = \sqrt{< \widehat{f}, \widehat{f} >}$
- for a binary boolean function from $\mathbb{Z}_2^n$ this norm is always $2^{n/2}$

Various definitions (cont.)

- **Def.: Real-valued counterpart of a binary boolean function f is defined as $\widehat{f}(u) = (-1)^{f(u)}$**
- $\widehat{f(a) \oplus g(a)} = \widehat{f}(a)\widehat{g}(a)$
- **Def.: Inner product** $< \widehat{f}, \widehat{g} >= \sum \widehat{f}(a)\widehat{g}(a)$
- this inner product defines a norm $\|\widehat{f}\| = \sqrt{< \widehat{f}, \widehat{f} >}$
- for a binary boolean function from $\mathbb{Z}_2^n$ this norm is always $2^{n/2}$

Correlation of two binary boolean functions

- Definition by probability
  $C(f(a), g(a)) = 2Prob[f(c) = g(c)] - 1$
- Definition by inner product
  $C(f(a), g(a)) = \frac{<\widehat{f}(a), \widehat{g}(a)>}{\|\widehat{f}\| \cdot \|\widehat{g}\|}$
- Definition by distance
  $C(f(a), g(a)) = 1 - \frac{d(f,g)}{2^{n-1}}$

Correlation of two binary boolean functions

- Definition by probability
  $C(f(a), g(a)) = 2Prob[f(c) = g(c)] - 1$
- Definition by inner product
  $C(f(a), g(a)) = \frac{<\widehat{f}(a), \widehat{g}(a)>}{\|\widehat{f}\| \cdot \|\widehat{g}\|}$
- Definition by distance
  $C(f(a), g(a)) = 1 - \frac{d(f,g)}{2^{n-1}}$

Correlation of two binary boolean functions

- Definition by probability
  $C(f(a), g(a)) = 2Prob[f(c) = g(c)] - 1$
- Definition by inner product
  $C(f(a), g(a)) = \frac{<\widehat{f}(a), \widehat{g}(a)>}{\|\widehat{f}\| \cdot \|\widehat{g}\|}$
- Definition by distance
  $C(f(a), g(a)) = 1 - \frac{d(f,g)}{2^{n-1}}$

Walsh-Hadamard spectrum

- every binary boolean function can be seen as a vector of a vector space $\mathbb{R}^{2^n}$ f $((-1)^{f(a_1)}, (-1)^{f(a_2)}, ..., (-1)^{f(a_{2^n})})$
- recall: there are 2^n parities on $\mathbb{Z}_2^n$
- fact: vectors corresponding to all parities form an orthogonal basis of $\mathbb{R}^{2^n}$

Walsh-Hadamard spectrum

- every binary boolean function can be seen as a vector of a vector space $\mathbb{R}^{2^n}$ f $((-1)^{f(a_1)}, (-1)^{f(a_2)}, ..., (-1)^{f(a_{2^n})})$
- recall: there are 2^n parities on $\mathbb{Z}_2^n$
- fact: vectors corresponding to all parities form an orthogonal basis of $\mathbb{R}^{2^n}$

Walsh-Hadamard spectrum

- every binary boolean function can be seen as a vector of a vector space $\mathbb{R}^{2^n}$ f $((-1)^{f(a_1)}, (-1)^{f(a_2)}, ..., (-1)^{f(a_{2^n})})$
- recall: there are 2^n parities on $\mathbb{Z}_2^n$
- fact: vectors corresponding to all parities form an orthogonal basis of $\mathbb{R}^{2^n}$

Walsh-Hadamard spectrum (cont.)

- **Def.: Walsh-Hadamard spectrum of a binary boolean function is the representation of the function with respect to the parity basis.**
- $\widehat{f}(a) = \sum_w F(w)(-1)^{w^T a}$
- $F(w) = C(f(a), w^T a)$
- Obviously, the spectrum F completely determines the function $\widehat{f}$(and f).

Walsh-Hadamard spectrum (cont.)

- **Def.: Walsh-Hadamard spectrum of a binary boolean function is the representation of the function with respect to the parity basis.**
- $\widehat{f}(a) = \sum_w F(w)(-1)^{w^T a}$
- $F(w) = C(f(a), w^T a)$
- Obviously, the spectrum F completely determines the function $\widehat{f}$(and f).

Walsh-Hadamard spectrum (cont.)

- **Def.: Walsh-Hadamard spectrum of a binary boolean function is the representation of the function with respect to the parity basis.**
- $\widehat{f}(a) = \sum_w F(w)(-1)^{w^T a}$
- $F(w) = C(f(a), w^T a)$
- Obviously, the spectrum F completely determines the function $\widehat{f}$(and f).

Walsh-Hadamard spectrum (cont.)

- **Def.: Walsh-Hadamard spectrum of a binary boolean function is the representation of the function with respect to the parity basis.**
- $\widehat{f}(a) = \sum_w F(w)(-1)^{w^T a}$
- $F(w) = C(f(a), w^T a)$
- Obviously, the spectrum F completely determines the function $\widehat{f}$(and f).

Parseval Theorem

- **Th.: For Walsh-Hadamard spectrum of a function $\widehat{f}$ (and f), the following holds:**
  $\sum_w F(w)^2 = 1$
- **Proof:** see the whiteboard

Parseval Theorem

- **Th.: For Walsh-Hadamard spectrum of a function $\widehat{f}$ (and f), the following holds:**
  $\sum_w F(w)^2 = 1$
- **Proof:** see the whiteboard

Examples of a spectrum

Please keep watching the whiteboard...

Correlation Matrix

- **Def.: Correlation matrix $C^{(h)}$ of a function h is a matrix $2^m x 2^n$ (with columns indexed by elements of $\mathbb{Z}_2^n$ and rows indexed by elements of $\mathbb{Z}_2^m$), where $C^{(h)}_{u,v} = C(u^T h(a), v^T a)$.**
- ...it is a matrix of correlations between input parities and output parities...
- ...rows are spectra of output parities...
- row u of $C^{(h)}$ can be seen as an expression of an output parity with respect to input parities $(-1)^{u^T h(a)} = \sum_w C^{(h)}_{u,w}(-1)^{wTa}$

Correlation Matrix

- **Def.: Correlation matrix $C^{(h)}$ of a function h is a matrix $2^m x 2^n$ (with columns indexed by elements of $\mathbb{Z}_2^n$ and rows indexed by elements of $\mathbb{Z}_2^m$), where $C^{(h)}_{u,v} = C(u^T h(a), v^T a)$.**
- ...it is a matrix of correlations between input parities and output parities...
- ...rows are spectra of output parities...
- row u of $C^{(h)}$ can be seen as an expression of an output parity with respect to input parities $(-1)^{u^T h(a)} = \sum_w C^{(h)}_{u,w}(-1)^{wTa}$

Correlation Matrix

- **Def.: Correlation matrix $C^{(h)}$ of a function h is a matrix $2^m x 2^n$ (with columns indexed by elements of $\mathbb{Z}_2^n$ and rows indexed by elements of $\mathbb{Z}_2^m$), where $C^{(h)}_{u,v} = C(u^T h(a), v^T a)$.**
- ...it is a matrix of correlations between input parities and output parities...
- ...rows are spectra of output parities...
- row u of $C^{(h)}$ can be seen as an expression of an output parity with respect to input parities $(-1)^{u^T h(a)} = \sum_w C^{(h)}_{u,w}(-1)^{wTa}$

Correlation Matrix

- **Def.: Correlation matrix $C^{(h)}$ of a function h is a matrix $2^m x 2^n$ (with columns indexed by elements of $\mathbb{Z}_2^n$ and rows indexed by elements of $\mathbb{Z}_2^m$), where $C^{(h)}_{u,v} = C(u^T h(a), v^T a)$.**
- ...it is a matrix of correlations between input parities and output parities...
- ...rows are spectra of output parities...
- row u of $C^{(h)}$ can be seen as an expression of an output parity with respect to input parities $(-1)^{u^T h(a)} = \sum_w C^{(h)}_{u,w}(-1)^{wTa}$

Example of an invertible boolean transformation $f : \mathbb{Z}_2^3 \to \mathbb{Z}_2^3$

a_1	a_2	a_3	$f_1(a_1, a_2, a_3)$	$f_2(a_1, a_2, a_3)$	$f_3(a_1, a_2, a_3)$
0	0	0	0	1	0
1	0	0	0	1	1
0	1	0	0	0	1
1	1	0	1	0	0
0	0	1	1	1	1
1	0	1	0	0	0
0	1	1	1	1	0
1	1	1	1	0	1

Algebraic normal form of this transformation is:

$$f_1(a_1, a_2, a_3) = a_3 + a_1a_2 + a_1a_3,$$
$$f_2(a_1, a_2, a_3) = 1 + a_2 + a_1a_3 + a_2a_3,$$
$$f_2(a_1, a_2, a_3) = a_1 + a_2 + a_3.$$

List of all parity functions $f : \mathbb{Z}_2^3 \to \mathbb{Z}_2$

0	a_1	a_2	$a_1 + a_2$	a_3	$a_1 + a_3$	$a_2 + a_3$	$a_1 + a_2 + a_3$
0	0	0	0	0	0	0	0
0	1	0	1	0	1	0	1
0	0	1	0	0	0	1	1
0	1	1	0	0	1	1	0
0	0	0	0	1	1	1	1
0	1	0	1	1	0	1	0
0	0	1	1	1	1	0	0
0	1	1	0	1	0	0	1

Correlation matrix of $f : \mathbb{Z}_2^3 \to \mathbb{Z}_2^3$

	0	a_1	a_2	$a_1 + a_2$	a_3	$a_1 + a_3$	$a_2 + a_3$	$a_1 + a_2 + a_3$
0	1	0	0	0	0	0	0	0
f_1	0	0	$\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{2}$	0	0
f_2	0	$-\frac{1}{2}$	$-\frac{1}{2}$	0	0	$\frac{1}{2}$	$-\frac{1}{2}$	0
$f_1 + f_2$	0	$\frac{1}{2}$	0	$-\frac{1}{2}$	$-\frac{1}{2}$	0	$-\frac{1}{2}$	0
f_3	0	0	0	0	0	0	0	1
$f_1 + f_3$	0	0	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	0	0
$f_2 + f_3$	0	$-\frac{1}{2}$	$\frac{1}{2}$	0	0	$-\frac{1}{2}$	$-\frac{1}{2}$	0
$f_1 + f_2 + f_3$	0	$-\frac{1}{2}$	0	$-\frac{1}{2}$	$-\frac{1}{2}$	0	$\frac{1}{2}$	0

Basic properties of Correlation Matrices

- **If we have functions $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^p$, $g : \mathbb{Z}_2^p \to \mathbb{Z}_2^m$ and $h : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ s.t. $h = g \circ f$, then $C^{(h)} = C^{(g)} C^{(f)}$**
- Why?
- If we define $f : \mathbb{Z}_2^n \to \mathbb{R}^{2^n}$
  $f(a) \to ((-1)^{u_1^T a}, (-1)^{u_2^T a}, ..., (-1)^{u_{2^n}^T a})$,
  (binary vector $a \to$ values of all parities on a),
  then L is a group homomorphism of $< \mathbb{Z}_2^n, \oplus >$ and
  $< \mathbb{R}^{2^n} \setminus \{0\}, \cdot >$,
- and from $(-1)^{u^T h(a)} = \sum_w C_{u,w}^{(h)} (-1)^{w^T a}$ it follows that $C^{(h)} \cdot L(a)^T = L(h(a))$, so there is a correspondence between applying a boolean function h on a vector a and multiplying $L(a)$ with $C^{(h)}$.
- (see the whiteboard for a picture that clarifies the rest)

Basic properties of Correlation Matrices

- **If we have functions $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^p$, $g : \mathbb{Z}_2^p \to \mathbb{Z}_2^m$ and $h : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ s.t. $h = g \circ f$, then $C^{(h)} = C^{(g)} C^{(f)}$**
- Why?
- If we define $f : \mathbb{Z}_2^n \to \mathbb{R}^{2^n}$
  $f(a) \to ((-1)^{u_1^T a}, (-1)^{u_2^T a}, ..., (-1)^{u_{2^n}^T a})$,
  (binary vector $a \to$ values of all parities on a),
  then L is a group homomorphism of $< \mathbb{Z}_2^n, \oplus >$ and
  $< \mathbb{R}^{2^n} \setminus \{0\}, \cdot >$,
- and from $(-1)^{u^T h(a)} = \sum_w C_{u,w}^{(h)} (-1)^{w^T a}$ it follows that $C^{(h)} \cdot L(a)^T = L(h(a))$, so there is a correspondence between applying a boolean function h on a vector a and multiplying $L(a)$ with $C^{(h)}$.
- (see the whiteboard for a picture that clarifies the rest)

Basic properties of Correlation Matrices

- **If we have functions** $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^p$, $g : \mathbb{Z}_2^p \to \mathbb{Z}_2^m$ **and** $h : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ **s.t.** $h = g \circ f$**, then** $C^{(h)} = C^{(g)} C^{(f)}$
- Why?
- If we define $f : \mathbb{Z}_2^n \to \mathbb{R}^{2^n}$
  $f(a) \to ((-1)^{u_1^T a}, (-1)^{u_2^T a}, ..., (-1)^{u_{2^n}^T a})$,
  (binary vector $a \to$ values of all parities on a),
  then L is a group homomorphism of $< \mathbb{Z}_2^n, \oplus >$ and
  $< \mathbb{R}^{2^n} \setminus \{0\}, \cdot >$,
- and from $(-1)^{u^T h(a)} = \sum_w C_{u,w}^{(h)} (-1)^{w^T a}$ it follows that $C^{(h)} \cdot L(a)^T = L(h(a))$, so there is a correspondence between applying a boolean function h on a vector a and multiplying $L(a)$ with $C^{(h)}$.
- (see the whiteboard for a picture that clarifies the rest)

Basic properties of Correlation Matrices

- **If we have functions** $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^p$, $g : \mathbb{Z}_2^p \to \mathbb{Z}_2^m$ **and** $h : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ **s.t.** $h = g \circ f$**, then** $C^{(h)} = C^{(g)} C^{(f)}$
- Why?
- If we define $f : \mathbb{Z}_2^n \to \mathbb{R}^{2^n}$
  $f(a) \to ((-1)^{u_1^T a}, (-1)^{u_2^T a}, ..., (-1)^{u_{2^n}^T a})$,
  (binary vector $a \to$ values of all parities on a),
  then L is a group homomorphism of $< \mathbb{Z}_2^n, \oplus >$ and
  $< \mathbb{R}^{2^n} \setminus \{0\}, \cdot >$,
- and from $(-1)^{u^T h(a)} = \sum_w C_{u,w}^{(h)} (-1)^{w^T a}$ it follows that $C^{(h)} \cdot L(a)^T = L(h(a))$, so there is a correspondence between applying a boolean function h on a vector a and multiplying $L(a)$ with $C^{(h)}$.
- (see the whiteboard for a picture that clarifies the rest)

Basic properties of Correlation Matrices

- **If we have functions** $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^p$, $g : \mathbb{Z}_2^p \to \mathbb{Z}_2^m$ **and** $h : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ **s.t.** $h = g \circ f$**, then** $C^{(h)} = C^{(g)} C^{(f)}$
- Why?
- If we define $f : \mathbb{Z}_2^n \to \mathbb{R}^{2^n}$
  $f(a) \to ((-1)^{u_1^T a}, (-1)^{u_2^T a}, ..., (-1)^{u_{2^n}^T a})$,
  (binary vector $a \to$ values of all parities on a),
  then L is a group homomorphism of $< \mathbb{Z}_2^n, \oplus >$ and
  $< \mathbb{R}^{2^n} \setminus \{0\}, \cdot >$,
- and from $(-1)^{u^T h(a)} = \sum_w C_{u,w}^{(h)} (-1)^{w^T a}$ it follows that $C^{(h)} \cdot L(a)^T = L(h(a))$, so there is a correspondence between applying a boolean function h on a vector a and multiplying $L(a)$ with $C^{(h)}$.
- (see the whiteboard for a picture that clarifies the rest)

Boolean Permutation and Invertibility of Correlation Matrix

Let $h : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ be a boolean permutation. Then following holds:

- $C^{(h)}$ **is invertible.**
- $h \circ h^{-1} = id = h^{-1} \circ h$, so $C^{(h)} \cdot C^{(h^{-1})} = I = C^{(h^{-1})} \cdot C^{(h)}$ and therefore $C^{(h)-1} = C^{(h^{-1})}$.
- Note: the opposite implication ($C^{(h)}$ invertible $\Longrightarrow$ h invertible) also holds, but the proof needs more calculations

Boolean Permutation and Invertibility of Correlation Matrix

Let $h : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ be a boolean permutation. Then following holds:

- $C^{(h)}$ **is invertible.**
- $h \circ h^{-1} = id = h^{-1} \circ h$, so $C^{(h)} \cdot C^{(h^{-1})} = I = C^{(h^{-1})} \cdot C^{(h)}$ and therefore $C^{(h)-1} = C^{(h^{-1})}$.
- Note: the opposite implication ($C^{(h)}$ invertible $\Longrightarrow$ h invertible) also holds, but the proof needs more calculations

Boolean Permutation and Invertibility of Correlation Matrix

Let $h : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ be a boolean permutation. Then following holds:

- $C^{(h)}$ **is invertible.**
- $h \circ h^{-1} = id = h^{-1} \circ h$, so $C^{(h)} \cdot C^{(h^{-1})} = I = C^{(h^{-1})} \cdot C^{(h)}$ and therefore $C^{(h)-1} = C^{(h^{-1})}$.
- Note: the opposite implication ($C^{(h)}$ invertible $\Longrightarrow$ h invertible) also holds, but the proof needs more calculations

Boolean Permutation and Invertibility of Correlation Matrix (cont.)

- $C^{(h)-1} = C^{(h)T}$, **in other words,** $C^{(h)}$ **is orthogonal.**
- (see the whiteboard for the easy calculations, for the last time)

Boolean Permutation and Invertibility of Correlation Matrix (cont.)

- $C^{(h)-1} = C^{(h)T}$, **in other words,** $C^{(h)}$ **is orthogonal.**
- (see the whiteboard for the easy calculations, for the last time)

It's over

Thanks:)