J Appl Math Comput manuscript No.
(will be inserted by the editor)

Dirichlet Product for Boolean Functions

Abderrahmane Nitaj · Willy Susilo · Joseph Tonien

Received: date / Accepted: date

Abstract Boolean functions play an important role in many symmetric cryptosystems and are crucial for their security. It is important to design boolean functions with reliable cryptographic properties such as balancedness and nonlinearity. Most of these properties are based on specific structures such as Möbius transform and Algebraic Normal Form. In this paper, we introduce the notion of Dirichlet product and use it to study the arithmetical properties of boolean functions. We show that, with the Dirichlet product, the set of boolean functions is an Abelian monoid with interesting algebraic structure. In addition, we apply the Dirichlet product to the sub-family of coincident functions and exhibit many properties satisfied by such functions.

Keywords Boolean Functions, Möbius Transform, Dirichlet Product, Coincident Functions

1 Introduction

Boolean functions are used in logic and in many cryptographic applications such as blocks of symmetric key cryptosystems, stream cipher systems, coding theory and hash functions. Boolean functions are important for the security of such systems. So, for security reason, one seeks boolean functions having good properties such as nonlinearity, balancedness and algebraic immunity [7,4] (see [3] for more properties). A boolean function is a mapping $\{0,1\}^n \to \{0,1\}$, often characterized by its truth table. The number of boolean functions with n variables is 2^{2^n} and it is impracticable to exhaustively exhibit a boolean function with optimal properties. One way to tackle this problem is to study the arithmetical structure of boolean functions and test their

Abderrahmane Nitaj
Laboratoire de Mathématiques Nicolas Oresme, Université de Caen Normandie, France
E-mail: abderrahmane.nitaj@unicaen.fr

Willy Susilo · Joseph Tonien
Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, Australia
E-mail: wsusilo@uow.edu.au, joseph_tonien@uow.edu.au

cryptographic reliability by the mean of algebraic tools such as Möbius transform and Algebraic Normal Form. For this reason, a lot of effort has been given to find ways to construct boolean functions with strong cryptographic properties.

For $n \geq 1$, we set $GF(2) = \{0, 1\}$ and $GF(2)^n = \{0, 1\}^n$. Any vector $x \in GF(2)^n$ is represented by its coordinates as $x = (x_1, \ldots, x_n)$ or simply $x = x_1 \ldots x_n$. The Hamming weight $w_H(x)$ of $x \in GF(2)^n$ is the number of non zero coordinates of x. An n-boolean function f is a mapping from $GF(2)^n$ into $GF(2)$. A boolean function is completely determined by its truth table

$$f(0,0,0\ldots,0), f(0,1,0,\ldots,0), f(0,1,0,\ldots,0), \ldots, f(1,1,1,\ldots,1),$$

and can be represented uniquely by the algebraic normal form (ANF)

$$f(x_1, \ldots, x_n) = \sum_{(\epsilon_1,\ldots,\epsilon_n) \in GF(2)^n} \hat{f}(\epsilon_1, \ldots, \epsilon_n) x_1^{\epsilon_1} \ldots x_n^{\epsilon_n},$$

where $\hat{f}$ is also a boolean function, called the Möbius transform of f. The transformation of f to its ANF can be performed using the truth table of f (see [2] and [6]).

Boolean functions have been intensively studied and various arithmetical properties are known such as Möbius transforms [6], Fourier transforms [2] and some cryptographic applications [7]. In this paper, we improve much further such arithmetic properties by introducing the concept of *Dirichlet product*. Usually, Dirichlet product is well defined for arithmetical functions. An arithmetical function is a real-valued function defined on the positive integers [1]. The classical Dirichlet product $F * G$ for two arithmetical functions $F, G : \mathbb{N} \to \mathbb{R}$ is defined by

$$(F * G)(n) = \sum_{d|n} F(d) G(\frac{n}{d}) = \sum_{xy=n} F(x) G(y).$$

Dirichlet product is commutative $F*G = G*F$, associative $F*(G*H) = (F*G)*H$, and it has an identity

$$I(n) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } n > 1 \end{cases} \tag{1}$$

where $F*I = I*F = F$. So the set of all arithmetical functions $\mathbb{N} \to \mathbb{R}$ together with the Dirichlet product form an Abelian monoid. What more is that if $F(1) \neq 0$ then F has an inverse. So the subset of all arithmetical functions such that $F(1) \neq 0$ is an Abelian group with respect to the Dirichlet multiplication. The classical Dirichlet product provides great inside into some of the classical theorems in number theory. Many identities involving the Möbius function μ and the Euler totient function ϕ can be seen more intuitively in the language of Dirichlet product. For example, we have this identity

$$\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } n > 1 \end{cases} \tag{2}$$

where μ is the the Möbius function

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n = p_1 \cdot p_2 \cdots p_k \\ 0 & \text{otherwise.} \end{cases}$$

In the language of Dirichlet product, the identity (2) is $\mu * 1 = I$, it means that the Möbius function μ is the Dirichlet inverse of the constant function 1 where $1(n) = 1$. Similarly, Euler's totient function satisfies the following result.

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}, \tag{3}$$

In the language of Dirichlet product, the identity (3) is $\mu * N = \phi$ where N is the function $N(n) = n$. In the language of group theory, it implies that $N = \phi * \mu^{-1} = \phi * 1$, that is

$$\sum_{d|n} \phi(d) = n. \tag{4}$$

So under the notion of Dirichlet product, two isolated results, (3) and (4) are ultimately related: (3) means $\phi = \mu * N$, whereas (4) means $N = \phi * 1 = \phi * \mu^{-1}$.

For two boolean functions f and g, we define the concept of Dirichlet product by setting for all $x \in GF(2)^n$

$$(f * g)(x) = \sum_{u \preceq x} f(u)g(x - u)$$

where, for $u = (u_1, \ldots, u_n) \in GF(2)^n$ and $x = (x_1, \ldots, x_n) \in GF(2)^n$, $u \preceq x$ if and only if for each $i \in \{1, \ldots, n\}$, $u_i \leq x_i$. We show that the Dirichlet product for boolean functions is commutative, associative and that the set of all boolean functions is an Abelian monoid and has the identity function I satisfying

$$I(x) = \begin{cases} 1 \text{ if } x = 0 \\ 0 \text{ if } x \neq 0 \end{cases}$$

Moreover, we link a boolean function f to its Möbius transform $\hat{f}$ using the Dirichlet products $f = \hat{f} * 1$ and $\hat{f} = f * 1$ where 1 is the constant function $1(x) = 1$. We show that the set of all boolean functions f such that $f(0, 0, \ldots, 0) = 1$ under the Dirichlet product form an Abelian group and the inverse of any such function f is f itself.

Finally, we will study the set of coincident functions and its algebraic structure. A coincident function is a boolean function f such that $\hat{f} = f$. Under the Dirichlet product, we show that the set of all coincident functions is a 2^{n-1} subspace with cardinality $2^{2^{n-1}}$.

The rest of this paper is organized as follows. In Section 2, we review the basic properties of boolean functions. In Section 3, we introduce the new notion of Dirichlet product for boolean functions and study its arithmetic properties. In Section 4, we study the arithmetical and algebraic structure of the set of all coincident boolean functions. We conclude the paper in Section 5.

2 Boolean functions

Let $n \geq 1$. A boolean function f on n variables is a mapping from $\{0, 1\}^n$ into $\{0, 1\}$. It can be defined by its truth table, that is by $f(x_1, \ldots, x_n)$ for each $(x_1, \ldots, x_n) \in$

$\{0,1\}^n$. For $x_i, \epsilon_i \in GF(2)$, we define $x_i^{\epsilon_i}$

$$x_i^{\epsilon_i} = \begin{cases} x_i & \text{if } \epsilon_i = 1, \\ 1 & \text{if } \epsilon_i = 0 \end{cases}$$

with the convention that $0^0 = 1$.

The set of all boolean functions on n variables is denoted $\mathcal{B}_n$ and any boolean function $f \in \mathcal{B}_n$ can be uniquely represented by an n-multivariate polynomial over $GF(2)$, called *algebraic normal form* (ANF),

$$f(x) = \sum_{\epsilon \in GF(2)^n} f_\epsilon \, x^\epsilon,$$

where $f_\epsilon \in GF(2)$ is the coefficient of the term $x^\epsilon = x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n}$. In $GF(2)$, the addition operation is simply the XOR.

The summand $x^\epsilon = x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$ is called a monomial (term) in the ANF of f. The summand x^ϵ is said to appear in f if $f_\epsilon \neq 0$. The degree of this summand x^ϵ is the Hamming weight $w_H(\epsilon)$ of ϵ, that is the number of non-zero elements in it. The (*algebraic*) degree of f, denoted by $\deg(f)$, is the maximum degree of all summands that appear in f, that is maximum of all Hamming weights. For a constant zero function, we assume its degree is 0. The coefficient f_ϵ of the summand x^ϵ is related the Möbius transformation.

Definition 1 Let $f \in \mathcal{B}_n$ with a polynomial

$$f(x) = \sum_{\epsilon \in GF(2)^n} f_\epsilon \, x^\epsilon.$$

The *Möbius transformation* of f is the boolean function $\hat{f} : GF(2)^n \to GF(2)$ defined as

$$\hat{f}(\epsilon) = f_\epsilon.$$

Using this definition, the polynomial $f(x)$ becomes

$$f(x) = \sum_{\epsilon \in GF(2)^n} \hat{f}(\epsilon) \, x^\epsilon.$$

We now define a partial ordering $\preceq$ in $GF(2)^n$ in the following definition.

Definition 2 Let $u = (u_1, u_2, \dots, u_n) \in GF(2)^n$ and $x = (x_1, x_2, \dots, x_n) \in GF(2)^n$. We define the ordering

$$u \preceq x \Leftrightarrow u_i \leq x_i \quad \text{for all} \quad i \quad \text{with} \quad 1 \leq i \leq n.$$

The following simple result gives an expression of a boolean function f in terms of its Möbius transform $\hat{f}$.

Theorem 1 *For $x = (x_1, \dots, x_n) \in GF(2)^n$ and $u = (u_1, \dots, u_n) \in GF(2)^n$,*

$$f(x) = \sum_{u \preceq x} \hat{f}(u), \tag{5}$$

Take an example, let $n = 3$,

$$f(x_1, x_2, x_3) = \hat{f}(0,0,0) + \hat{f}(1,0,0)x_1 + \hat{f}(0,1,0)x_2 + \hat{f}(0,0,1)x_3 + \hat{f}(1,1,0)x_1x_2 + \hat{f}(0,1,1)x_2x_3 + \hat{f}(1,0,1)x_1x_3 + \hat{f}(1,1,1)x_1x_2x_3.$$

So

$$\begin{aligned} f(0,0,0) &= \hat{f}(0,0,0) \\ f(1,0,0) &= \hat{f}(0,0,0) + \hat{f}(1,0,0) \\ f(0,1,0) &= \hat{f}(0,0,0) + \hat{f}(0,1,0) \\ f(0,0,1) &= \hat{f}(0,0,0) + \hat{f}(0,0,1) \\ f(1,1,0) &= \hat{f}(0,0,0) + \hat{f}(1,0,0) + \hat{f}(0,1,0) + \hat{f}(1,1,0) \\ &\dots \end{aligned}$$

Solving these equations, we have the dual equations

$$\begin{aligned} \hat{f}(0,0,0) &= f(0,0,0) \\ \hat{f}(1,0,0) &= f(0,0,0) + f(1,0,0) \\ \hat{f}(0,1,0) &= f(0,0,0) + f(0,1,0) \\ \hat{f}(0,0,1) &= f(0,0,0) + f(0,0,1) \\ \hat{f}(1,1,0) &= f(0,0,0) + f(1,0,0) + f(0,1,0) + f(1,1,0) \\ &\dots \end{aligned}$$

In matrix form, these equations become

$$\begin{pmatrix} f(0,0,0) \\ f(1,0,0) \\ f(0,1,0) \\ f(0,0,1) \\ f(1,1,0) \\ f(1,0,1) \\ f(0,1,1) \\ f(1,1,1) \end{pmatrix} = \begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 1&1&0&0&0&0&0&0 \\ 1&0&1&0&0&0&0&0 \\ 1&0&0&1&0&0&0&0 \\ 1&1&1&0&1&0&0&0 \\ 1&1&0&1&0&1&0&0 \\ 1&0&1&1&0&0&1&0 \\ 1&1&1&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} \hat{f}(0,0,0) \\ \hat{f}(1,0,0) \\ \hat{f}(0,1,0) \\ \hat{f}(0,0,1) \\ \hat{f}(1,1,0) \\ \hat{f}(1,0,1) \\ \hat{f}(0,1,1) \\ \hat{f}(1,1,1) \end{pmatrix}, \tag{6}$$

and

$$\begin{pmatrix} \hat{f}(0,0,0) \\ \hat{f}(1,0,0) \\ \hat{f}(0,1,0) \\ \hat{f}(0,0,1) \\ \hat{f}(1,1,0) \\ \hat{f}(1,0,1) \\ \hat{f}(0,1,1) \\ \hat{f}(1,1,1) \end{pmatrix} = \begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 1&1&0&0&0&0&0&0 \\ 1&0&1&0&0&0&0&0 \\ 1&0&0&1&0&0&0&0 \\ 1&1&1&0&1&0&0&0 \\ 1&1&0&1&0&1&0&0 \\ 1&0&1&1&0&0&1&0 \\ 1&1&1&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} f(0,0,0) \\ f(1,0,0) \\ f(0,1,0) \\ f(0,0,1) \\ f(1,1,0) \\ f(1,0,1) \\ f(0,1,1) \\ f(1,1,1) \end{pmatrix}. \tag{7}$$

In the above example, we can see the duality between f and $\hat{f}$

$$\hat{f}(x) = \sum_{u \preceq x} f(u). \tag{8}$$

This is not accidental. The duality between (5) and (8) is explained by the fact that $\hat{f} = f * 1$ and $f = \hat{f} * 1$ as in Theorem 3.

3 Dirichlet product for boolean functions

In this section, we define the Dirichlet product $f * g$ for two boolean functions f and g and study several properties of the monoid $(\mathcal{B}_n, *)$. In the rest of this paper, the term $(0, 0, \ldots, 0) \in GF(2)^n$ is often denoted as 0.

Lemma 1 *Let $x = (x_1, x_2, \ldots, x_n) \in GF(2)^n$. Then there are $2^{w_H(x)}$ terms $u = (u_1, u_2, \ldots, u_n) \in GF(2)^n$ such that $u \preceq x$ where $w_H(x)$ is the Hamming weight of x.*

Proof Let $x = (x_1, x_2, \ldots, x_n)$. For each i with $1 \leq i \leq n$, we have

$$u_i \leq x_i \quad \text{for} \quad \begin{cases} u_i = 0 & \text{if } x_i = 0 \\ u_i \in \{0, 1\} & \text{if } x_i = 1 \end{cases}$$

It follows that the number of terms $u \in GF(2)^n$ satisfying $u \preceq x$ is

$$\prod_{i=1}^{n} 2^{x_i} = 2^{w_H(x)},$$

$w_H(x)$ is the Hamming weight of x. □

Example 1 Let $n = 3$ and $x = (1, 0, 1) \in GF(2)^3$. Then the set of all $u \in GF(2)^3$ such that $u \preceq x$ is

$$\{(0, 0, 0), (0, 0, 1), (1, 0, 0), (1, 0, 1)\}.$$

Now, we define the notion of Dirichlet product of two boolean functions.

Definition 3 The Dirichlet product of two boolean functions $f, g \in \mathcal{B}_n$ is defined as

$$(f * g)(x) = \sum_{u \preceq x} f(u) g(x - u)$$

Example 2 Let $n = 3$ and $x = (0, 1, 1) \in GF(2)^3$. Let $f, g \in \mathcal{B}_3$. Then the Dirichlet product of f and g is

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

The following result shows that the set $\mathcal{B}_n$ is an abelian monoid with respect to the Dirichlet product.

Theorem 2 *$(\mathcal{B}_n, *)$ is an Abelian monoid with the identity*

$$I(x) = \begin{cases} 1 \text{ if } x = 0 \\ 0 \text{ if } x \neq 0 \end{cases} \tag{9}$$

Proof We have

$$\begin{aligned}(f*g)(x) &= \sum_{u\preceq x} f(u)g(x-u)\\ &= \sum_{u,v\preceq x, u+v=x} f(u)g(v)\\ &= \sum_{v\preceq x} g(v)f(x-v) = (g*f)(x),\end{aligned}$$

so the Dirichlet product is commutative: $f*g = g*f$.
We also have

$$((f*g)*h)(x) = \sum_{u,v,w\preceq x, u+v+w=x} f(u)g(v)h(w) = (f*(g*h))(x)$$

so the Dirichlet product is associative.
Finally,

$$(f*I)(x) = \sum_{u,v\preceq x, u+v=x} f(u)I(v) = f(x)I(0) = f(x),$$

and I is the identity. □

The following result shows that the Dirichlet product is distributive over the addition operation in $\mathcal{B}_n$.

Lemma 2 *For $f, g \in \mathcal{B}_n$, define addition operation $f+g \in \mathcal{B}_n$ as*

$$(f+g)(x) = f(x) + g(x).$$

Then the Dirichlet product is distributive over this addition operation.

Proof We have

$$(f*(g+h))(x) = \sum_{u\preceq x} f(u)(g+h)(x-u) = \sum_{u\preceq x} f(u)(g(x-u)+h(x-u))$$

$$= \sum_{u\preceq x} f(u)g(x-u) + \sum_{u\preceq x} f(u)h(x-u) = (f*g)(x) + (f*h)(x)$$

so $f*(g+h) = f*g + f*h$. □

The next result gives one of the basic properties of the Dirichlet product.

Lemma 3 *For any functions $f, g \in \mathcal{B}_n$,*

$$(f*g)(0) = f(0)g(0)$$

Proof Since $u \preceq 0$ happens only for $u = 0$, we have

$$(f*g)(0) = \sum_{u\preceq 0} f(u)g(0-u) = f(0)g(0).$$

□

The next result defines the constant boolean function 1 and links it to the identity function I.

Lemma 4 *Let $1 \in \mathcal{B}_n$ denote the constant function*

$$1(x) = 1, \quad \forall x \in GF(2)^n \tag{10}$$

then

$$1 * 1 = I.$$

It means that 1 is its own inverse under Dirichlet multiplication.

Proof By Theorem 3, we have $(1 * 1)(0) = 1(0)1(0) = 1$. For $x \neq 0$, we have

$$(1 * 1)(x) = \sum_{u \preceq x} 1(u)1(x-u) = \sum_{u \preceq x} 1.$$

Since, by Lemma 1, there are $2^{w_H(x)}$ terms u with $u \preceq x$, we have $(1 * 1)(x) = 0$ for $x \neq 0$. In conclusion, $1 * 1 = I$. □

The following result shows that the ANF of a boolean function is related to the Dirichlet product.

Theorem 3 *For any function $f \in \mathcal{B}_n$, we have*

$$f = \hat{f} * 1, \quad \hat{f} = f * 1, \quad \hat{\hat{f}} = f.$$

Proof First, we have

$$(\hat{f} * 1)(x) = \sum_{u \preceq x} \hat{f}(u)1(x-u) = \sum_{u \preceq x} \hat{f}(u).$$

Therefore, by Theorem 1, $f = \hat{f} * 1$.
Combining this with Lemma 4, we get

$$f * 1 = (\hat{f} * 1) * 1 = \hat{f} * (1 * 1) = \hat{f} * I = \hat{f}.$$

Applying the former results, we get

$$\hat{\hat{f}} = \hat{f} * 1 = (f * 1) * 1 = f * (1 * 1) = f * I = f.$$

This terminates the proof. □

The mysterious duality between a boolean function and its Möbius transformation is actually a manifestation of a simple fact in Dirichlet product, that is $1 * 1 = I$. The relationship between the results of Theorem 3 is liken to that of (3) and (4).

Theorem 4 *For any function $f \in \mathcal{B}_n$,*

$$\hat{f}(0) = f(0).$$

Proof The proof follows from Lemma 3 and Theorem 3. □

The following result shows that $f * f$ is either the identity I or the constant function 0.

Theorem 5 *For any function $f \in \mathcal{B}_n$,*

$$f * f = f(0)I = \begin{cases} I \text{ if } f(0) = 1 \\ 0 \text{ if } f(0) = 0 \end{cases} \tag{11}$$

Proof Applying Lemma 3, we get $(f * f)(0) = f(0)f(0) = f(0)$. When $x \neq 0$,

$$(f * f)(x) = \sum_{u \preceq x} f(u)f(x - u).$$

Since $u \preceq x$ and $x - u \preceq x$, everything in the sum appear twice. Hence, $(f * f)(x) = 0$. So $f * f = f(0)I$. □

Theorem 6 *For any function $f \in \mathcal{B}_n$,*

$$f * \hat{f} = \hat{f} * f = f(0), \tag{12}$$

where $f(0)$ is the constant function defined by $f(0)(x) = f(0)$.

Proof By Theorem 3 and Theorem 5, we have

$$f * \hat{f} = f * (f * 1) = (f * f) * 1 = f(0)I * 1 = f(0)1 = f(0),$$

□

In the following result, we give a characterization of a reversible boolean function with respect to the Dirichlet product.

Theorem 7 *For any function $f \in \mathcal{B}_n$, f has a Dirichlet inverse if and only if $f(0) = 1$, and in this case, f is the Dirichlet inverse of itself.*

Proof Suppose that f is invertible with an inverse g. Then $f * g = I$ and $(f * g)(0) = f(0)g(0) = 1$. Then $f(0) = 1$. Conversely, suppose that $f(0) = 1$, then $f * f = f(0)I = I$. Hence f is invertible and f is the Dirichlet inverse of itself. □

Next, we show that the set of Dirichlet invertible boolean functions is an Abelian group.

Theorem 8 *Let $\mathcal{B}_n^+$ denote the set*

$$\mathcal{B}_n^+ = \{f \in \mathcal{B}_n \ : \ f(0) = 1\}.$$

Then $(\mathcal{B}_n^+, *)$ is an Abelian group.

Proof Let $f \in \mathcal{B}_n^+$ and $g \in \mathcal{B}_n^+$ be two invertible boolean functions. By Theorem 7, we know that $f(0) = g(0) = 1$. Then $(f * g)(0) = f(0)g(0) = 1$, which implies that $f * g \in \mathcal{B}_n^+$. Moreover, the inverse of $f \in \mathcal{B}_n^+$ is itself and $\mathcal{B}_n^+$ contains the identity function I. These properties show that $(\mathcal{B}_n^+, *)$ is an Abelian subgroup of $(\mathcal{B}_n, *)$. □

The following result is related to the degree of boolean functions. Recall the degree of a boolean function f is defined as the maximum number of variables of the terms $x^\epsilon = x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n}$ in the ANF of f.

Theorem 9 *For any $f, g \in \mathcal{B}_n$, we have*

$$\deg(f) + \deg(g) \geq \deg(f * g * 1) \quad \textit{and} \quad \deg(f) + \deg(\hat{f}) \geq n.$$

Proof To prove the first assertion, first, if $\deg(f)+\deg(g) \geq n$ then this assertion is obviously true. We only need to prove it for the case $\deg(f)+\deg(g) < n$. If $w_H(x) > \deg(f)+\deg(g)$, then for any $u \preceq x$, $w_H(u)+w_H(x-u) = w(x) > \deg(f)+\deg(g)$, so $w_H(u) > \deg(f)$ or $w_H(x-u) > \deg(g)$. If $w_H(u) > \deg(f)$ then $\hat{f}(u) = 0$, and if $w_H(x-u) > \deg(g)$ then $\hat{g}(x-u) = 0$, so in either case, we have $\hat{f}(u)\hat{g}(x-u) = 0$. It follows that

$$(\hat{f} * \hat{g})(x) = \sum_{u \preceq x} \hat{f}(u)\hat{g}(x-u) = 0$$

holds for any $x \in GF(2)^n$ such that $w_H(x) > \deg(f)+\deg(g)$. Therefore,

$$\deg((\hat{f} * \hat{g}) * 1) \leq \deg(f)+\deg(g).$$

Finally, $(\hat{f}*\hat{g})*1 = f*1*g*1*1 = f*g*1$. This gives $\deg(f)+\deg(g) \geq \deg(f*g*1)$. Next, we have

$$\deg(f)+\deg(\hat{f}) \geq \deg(f * \hat{f} * 1).$$

But $f * \hat{f} * 1 = f * f * 1 * 1 = f(0)I * I = f(0)I = I$, so $\deg(f * \hat{f} * 1) = \deg(I) = n$ and we obtain the inequality $\deg(f)+\deg(\hat{f}) \geq n$. □

3.1 Basis for $(\mathcal{B}_n, +)$

For $f, g \in \mathcal{B}_n$, the function $f+g \in \mathcal{B}_n$ is defined as $(f+g)(x) = f(x)+g(x)$. With this addition operation, $\mathcal{B}_n$ is a free Abelian group. There are two natural ways to choose a basis for $\mathcal{B}_n$. We will describe them in Theorem 10 and Theorem 11.

Theorem 10 *For each $a \in GF(2)^n$, define the function $\delta_a \in \mathcal{B}_n$ as follows*

$$\delta_a(x) = (x_1+a_1+1)(x_2+a_2+1)\dots(x_n+a_n+1) = \begin{cases} 1 \text{ if } x = a \\ 0 \text{ if } x \neq a \end{cases} \tag{13}$$

Then $\{\delta_a\}_{a \in GF(2)^n}$ forms a basis for the vector space $(\mathcal{B}_n, +)$. Each function $f \in \mathcal{B}_n$ can be written as a linear combination of basis functions δ_a as

$$f = \sum_{a \in GF(2)^n} f(a)\ \delta_a. \tag{14}$$

Proof If $x = a$, then for each $i = 1, 2, \dots, n$, $x_i + a_i + 1 = 1$ and $\delta_a(x) = 1$. If $x \neq a$, then $x_i \neq a_i$ for some i. Hence $x_i + a_i + 1 = 0$ and $\delta_a(x) = 0$.

We have

$$\sum_{a \in GF(2)^n} f(a)\ \delta_a(x) = f(x)\ \delta_x(x) + \sum_{a \neq x} f(a)\ \delta_a(x) = f(x),$$

so $f = \sum_{a \in GF(2)^n} f(a)\ \delta_a$. □

Note that, δ_0 is the Dirichlet identity function I:

$$I(x) = \delta_0(x) = (x_1+1)(x_2+1)\dots(x_n+1) = \begin{cases} 1 \text{ if } x = 0 \\ 0 \text{ if } x \neq 0 \end{cases} \tag{15}$$

Theorem 11 *For each $a \in GF(2)^n$, define the function $\rho_a \in \mathcal{B}_n$ as follows*

$$\rho_a(x) = x^a = x_1^{a_1} x_2^{a_2} \dots x_n^{a_n} = \begin{cases} 1 \text{ if } a \preceq x \\ 0 \text{ if } a \not\preceq x \end{cases} \tag{16}$$

Then $\{\rho_a\}_{a \in GF(2)^n}$ forms a basis for the vector space $(\mathcal{B}_n, +)$. Each function $f \in \mathcal{B}_n$ can be written as a linear combination of basis functions ρ_a as

$$f = \sum_{a \in GF(2)^n} \hat{f}(a)\ \rho_a. \tag{17}$$

Proof If $a \preceq x$ then $a_i \leq x_i$ for each $i = 1, 2, \dots, n$. If $x_i = 0$, then $a_i = 0$ and $x_i^{a_i} = 0^0 = 1$. If $x_i = 1$, then $x_i^{a_i} = 1$. In all cases, $x_i^{a_i} = 1$ and $\rho_a(x) = 1$.
Next, suppose that $a \not\preceq x$. Then there exists i with $1 \leq i \leq n$ such that $a_i > x_i$. This implies that $x_i = 0$ and $a_i = 1$. Hence $x_i^{a_i} = x_i = 0$ and $\rho_a(x) = 0$.
Now, we have for $x \in GF(2)^n$,

$$\sum_{a \in GF(2)^n} \hat{f}(a)\ \rho_a(x) = \sum_{a \preceq x} \hat{f}(a)\ \rho_a(x) + \sum_{a \not\preceq x} \hat{f}(a)\ \rho_a(x) = \sum_{a \preceq x} \hat{f}(a) = f(x),$$

by Theorem 1. □

Theorem 12 *For any $a \in GF(2)^n$, the basis functions δ_a and ρ_a satisfy the following relations:*

- $\delta_a * 1 = \rho_a$ *and* $\rho_a * 1 = \delta_a$,
- $\delta_a * \delta_b = \rho_a * \rho_b = \rho_a\, \rho_b\, \delta_{a+b}$.

Proof First, observe that since $\rho_a(x) = x^a$, the function ρ_a in ANF has only one monomial term x^a, so its ANF coefficient function is δ_a. That is $\rho_a * 1 = \delta_a$, and so $\delta_a * 1 = \rho_a * 1 * 1 = \delta_a * I = \delta_a$.
Next, for any a and b, we have

$$\begin{aligned} (\delta_a * \delta_b)(x) &= \sum_{u,v \preceq x, u+v=x} \delta_a(u)\delta_b(v) \\ &= \begin{cases} 1 & \text{if } a \preceq x,\ b \preceq x,\ a+b=x. \\ 0 & \text{otherwise} \end{cases} \\ &= \rho_a(x)\rho_b(x)\delta_{a+b}(x) \end{aligned}$$

Therefore,

$$\delta_a * \delta_b = \rho_a\, \rho_b\, \delta_{a+b}.$$

Finally,

$$\rho_a * \rho_b = \delta_a * 1 * \delta_b * 1 = \delta_a * \delta_b.$$

□

4 Coincident functions

In this section, we study a special family of boolean functions, called coincident functions which was first introduced in [5].

Definition 4 A coincident function is a function $f : GF(2)^n \to GF(2)$ such that $\hat{f} = f$.

Example 3 For $n = 3$, let f be the function

$$\begin{aligned} f(x_1, x_2, x_3) &= \hat{f}(0,0,0) + \hat{f}(1,0,0)x_1 + \hat{f}(0,1,0)x_2 + \hat{f}(0,0,1)x_3 + \\ &\quad \hat{f}(1,1,0)x_1x_2 + \hat{f}(0,1,1)x_2x_3 + \hat{f}(1,0,1)x_1x_3 + \hat{f}(1,1,1)x_1x_2x_3 \\ &= 0 + x_1 + x_2 + x_3 + x_1x_2 + x_2x_3 + x_1x_3 + x_1x_2x_3. \end{aligned}$$

Then

$$f(0,0,0) = \hat{f}(0,0,0) = 0, \quad f(1,0,0) = \hat{f}(1,0,0) = 1, \ldots, f(1,1,1) = \hat{f}(1,1,1) = 1,$$

that is $f = \hat{f}$ and f is coincident.

Theorem 13 *For any coincident function f,*

$$f(0) = 0.$$

Proof Suppose that f is a coincident function, that is $f = \hat{f}$. Then, using Theorem 1, we get

$$f(0,0,\ldots,0,1) = \hat{f}(0) + \hat{f}(0,0,\ldots,0,1).$$

Since $f(0,0,\ldots,0,1) = \hat{f}(0,0,\ldots,0,1)$, then $\hat{f}(0) = f(0) = 0$. □

Let $\mathcal{C}_n$ denote the set of all such coincident functions.

Theorem 14 *A function $f \in \mathcal{B}_n$ is a coincident function if and only if*

$$(1 + I) * f = 0.$$

Thus, $\mathcal{C}_n$ is the annihilator of $1 + I$ in $\mathcal{B}_n$.

Proof Suppose that f is a coincident function, that is $f = \hat{f}$. Then

$$0 = \hat{f} + f = f * 1 + f * I = f * (1 + I).$$

Conversely, suppose that $f*(1+I) = 0$. Then, using Theorem 3, we get $f*1+f*I = \hat{f} + f = 0$. This implies that $\hat{f} = f$ and then f is coincident. □

Observe that for any $x \in GF(2)^n$, we have

$$\begin{aligned} (1 + I)(x) &= (x_1 + 1)(x_2 + 1)\ldots(x_n + 1) + 1, \\ \delta_{1\ldots1}(x) &= x_1x_2\ldots x_n, \\ \rho_{1\ldots1}(x) &= x_1x_2\ldots x_n. \end{aligned}$$

Theorem 15 *The boolean functions $1 + I$, $\delta_{1\ldots1}$ and $\rho_{1\ldots1}$ are coincident functions.*

Proof Combining Theorem 14 and Theorem 4, we get

$$(1+I)*(1+I) = 1*1 + I*I = I + I = 0.$$

Hence $1+I$ is coincident. Next, combining Theorem 14 and Lemma 12, we get for any $x \in GF(2)^n$,

$$(1+I)*\delta_{1\ldots1}(x) = (1*\delta_{1\ldots1})(x) + (I*\delta_{1\ldots1})(x) = \rho_{1\ldots1}(x) + \delta_{1\ldots1}(x).$$

Then, using Theorem 10 and Theorem 11, we get

$$\rho_{1\ldots1}(x) + \delta_{1\ldots1}(x) = \begin{cases} 1+1=0 & \text{if } x = 1\ldots1, \\ 0+0=0 & \text{if } x \neq 1\ldots1. \end{cases}$$

It follows that $(1+I)*\delta_{1\ldots1} = 0$ and $\delta_{1\ldots1}$ is coincident. □

Theorem 16 *For any $u \in GF(2)^n$, $\delta_u + \rho_u$ is a coincident function.*

Proof Combining Theorem 14 and Theorem 12, we get

$$(1+I)*(\delta_u + \rho_u) = 1*\delta_u + 1*\rho_u + \delta_u + \rho_u = 2\delta_u + 2\rho_u = 0$$

Hence $\delta_u + \rho_u$ is a coincident function. □

Theorem 17 *A function $f \in \mathcal{B}_n$ is a coincident function if and only if for any $(x_2, \ldots, x_n) \in GF(2)^{n-1}$,*

$$f(0, x_2, \ldots, x_n) = \sum_{(u_2,\ldots,u_n) \prec (x_2,\ldots,x_n)} f(1, u_2, \ldots, u_n), \tag{18}$$

where $u \prec x$ means $u \preceq x$ and $u \neq x$.

Proof Since

$$(1+I)(x) = \begin{cases} 0 \text{ if } x = 0 \\ 1 \text{ if } x \neq 0 \end{cases} \tag{19}$$

we have

$$((1+I)*f)(x) = \sum_{u \preceq x} f(u)(1+I)(x-u) = \sum_{u \prec x} f(u).$$

Therefore, $(1+I)*f = 0$ if and only if for any $x \in GF(2)^n$,

$$\sum_{u \prec x} f(u) = 0.$$

Consider two cases, $x_1 = 0$ and $x_1 = 1$.
When $x_1 = 0$, the condition becomes

$$\sum_{(u_2,\ldots,u_n) \prec (x_2,\ldots,x_n)} f(0, u_2, \ldots, u_n) = 0.$$

When $x_1 = 1$, the condition becomes

$$f(0, x_2, \ldots, x_n) + \sum_{(u_2,\ldots,u_n) \prec (x_2,\ldots,x_n)} f(0, u_2, \ldots, u_n) + \sum_{(u_2,\ldots,u_n) \prec (x_2,\ldots,x_n)} f(1, u_2, \ldots, u_n) = 0.$$

Therefore, if f is a coincident function then for any $(x_2, \ldots, x_n) \in GF(2)^{n-1}$, we must have

$$f(0, x_2, \ldots, x_n) = \sum_{(u_2,\ldots,u_n) \prec (x_2,\ldots,x_n)} f(1, u_2, \ldots, u_n).$$

Conversely, suppose that for any $(x_2, \ldots, x_n) \in GF(2)^{n-1}$,

$$f(0, x_2, \ldots, x_n) = \sum_{(u_2,\ldots,u_n) \prec (x_2,\ldots,x_n)} f(1, u_2, \ldots, u_n).$$

Then

$$\sum_{(u_2,\ldots,u_n) \prec (x_2,\ldots,x_n)} f(0, u_2, \ldots, u_n) = \sum_{(u_2,\ldots,u_n) \prec (x_2,\ldots,x_n)} \sum_{(v_2,\ldots,v_n) \prec (u_2,\ldots,u_n)} f(1, v_2, \ldots, v_n).$$

The above sum is equal to 0 because for any term $f(1, v_2, \ldots, v_n)$, the number of its occurrences in the sum is equal to the number of $(u_2, \ldots, u_n)$ such that $(v_2, \ldots, v_n) \prec (u_2, \ldots, u_n) \prec (x_2, \ldots, x_n)$, and this is always an even number for any $(v_2, \ldots, v_n) \prec (x_2, \ldots, x_n)$. Hence for any $(x_2, \ldots, x_n) \in GF(2)^{n-1}$, we have

$$\sum_{(u_2,\ldots,u_n) \prec (x_2,\ldots,x_n)} f(0, u_2, \ldots, u_n) = 0. \tag{20}$$

Therefore,

$$f(0, x_2, \ldots, x_n) + \sum_{(u_2,\ldots,u_n) \prec (x_2,\ldots,x_n)} f(0, u_2, \ldots, u_n) + \sum_{(u_2,\ldots,u_n) \prec (x_2,\ldots,x_n)} f(1, u_2, \ldots, u_n) = 0. \tag{21}$$

Combining (20) and (21), we see that

$$\sum_{u \prec x} f(u) = 0,$$

that is $(1 + I) * f = 0$ and f is a coincident function. □

The following theorem reveals a relationship between the set of coincident functions $\mathcal{C}_n$ and the set of all boolean functions $\mathcal{B}_n$.

Theorem 18 *It holds that*

1. *A coincident function $f \in \mathcal{C}_n$ is specified freely and uniquely by its values on 2^{n-1} points $(1, u_2, \ldots, u_n) \in GF(2)^n$.*
2. *There are exactly $2^{2^{n-1}}$ coincident functions in total.*
3. *$(\mathcal{C}_n, +)$ is a 2^{n-1}-dimensional linear subspace of $(\mathcal{B}_n, +)$.*

Proof To prove the first assertion, observe that by Theorem 17, a coincident function $f \in \mathcal{C}_n$ is specified freely by its values on 2^{n-1} points $(1, u_2, \ldots, u_n) \in GF(2)^n$, and its values on 2^{n-1} other points $(0, u_2, \ldots, u_n) \in GF(2)^n$ are uniquely determined by (18). The second assertion follows since there are exactly 2 choices for choosing $f(1, u_2, \ldots, u_n) \in \{0, 1\}$, then there are exactly $2^{2^{n-1}}$ coincident functions in total. To prove the third assertion, observe that if $f \in \mathcal{C}_n$ and $g \in \mathcal{C}_n$, then $f + g \in \mathcal{C}_n$. On the other hand, the relation (18) defines any coincident function $f \in \mathcal{C}_n$. It follows that $(\mathcal{C}_n, +)$ is a 2^{n-1}-dimensional linear subspace of $(\mathcal{B}_n, +)$. □

4.1 Basis for $(\mathcal{C}_n, +)$

By Theorem 18, we know that $(\mathcal{C}_n, +)$ is a 2^{n-1}-dimensional linear subspace of $(\mathcal{B}_n, +)$. The following result gives an explicit basis for $(\mathcal{C}_n, +)$.

Theorem 19 *For each $(u_2, \ldots, u_n) \in GF(2)^{n-1}$, define the function $\gamma_{(u_2,\ldots,u_n)} \in \mathcal{B}_n$ as follows*

$$\gamma_{(u_2,\ldots,u_n)} = \delta_{(0,u_2,\ldots,u_n)} + \delta_{(1,u_2,\ldots,u_n)} + \rho_{(0,u_2,\ldots,u_n)} + \rho_{(1,u_2,\ldots,u_n)}$$

Then $\{\gamma_{(u_2,\ldots,u_n)}\}_{(u_2,\ldots,u_n)\in GF(2)^{n-1}}$ forms a basis for the subspace $(\mathcal{C}_n, +)$, and each coincident function $f \in \mathcal{C}_n$ can be written as a linear combination of basis functions as

$$f = \sum_{(u_2,\ldots,u_n)\in GF(2)^{n-1}} f(1, u_2, \ldots, u_n)\ \gamma_{(u_2,\ldots,u_n)}.$$

Proof A coincident function $f \in \mathcal{B}_n$ is specified freely and uniquely by its values on 2^{n-1} points $(1, u_2, \ldots, u_n) \in GF(2)^n$. For each $(u_2, \ldots, u_n) \in GF(2)^{n-1}$, define the coincident function $c_{(u_2,\ldots,u_n)} : GF(2)^n \to GF(2)$ as follows

$$c_{(u_2,\ldots,u_n)}(x) = \begin{cases} 1 \text{ if } (x_2, \ldots, x_n) = (u_2, \ldots, u_n) \\ 0 \text{ otherwise} \end{cases}$$

then the collection of these functions $c_{(u_2,\ldots,u_n)}$ will form a basis for the vector space $\mathcal{C}_n$ and

$$f = \sum_{(u_2,\ldots,u_n)\in GF(2)^{n-1}} f(1, u_2, \ldots, u_n)\ c_{(u_2,\ldots,u_n)}.$$

We need to show that

$$c_{(u_2,\ldots,u_n)} = \gamma_{(u_2,\ldots,u_n)}.$$

Indeed, by Theorem 16, $\gamma_{(u_2,\ldots,u_n)}$ is a coincident function, so it suffices to show that $\gamma_{(u_2,\ldots,u_n)}$ and $c_{(u_2,\ldots,u_n)}$ agree on 2^{n-1} points $(1, x_2, \ldots, x_n)$. We have

$$\delta_{(0,u_2,\ldots,u_n)}(1, x_2, \ldots, x_n) = 0$$

$$\delta_{(1,u_2,\ldots,u_n)}(1, x_2, \ldots, x_n) = \begin{cases} 1 \text{ if } (x_2, \ldots, x_n) = (u_2, \ldots, u_n) \\ 0 \text{ otherwise} \end{cases}$$

$$\rho_{(0,u_2,\ldots,u_n)}(1,x_2,\ldots,x_n)=\rho_{(1,u_2,\ldots,u_n)}(1,x_2,\ldots,x_n)$$

Therefore,

$$\gamma_{(u_2,\ldots,u_n)}(1,x_2,\ldots,x_n)=\begin{cases}1 \text{ if } (x_2,\ldots,x_n)=(u_2,\ldots,u_n)\\ 0 \text{ otherwise}\end{cases}$$

and thus, $\gamma_{(u_2,\ldots,u_n)}=c_{(u_2,\ldots,u_n)}$. □

Example 4 When $n=3$, the following 4 coincident functions form a basis for the subspace of all coincident functions:

$$\begin{aligned}\gamma_{(0,0)}&=\delta_{(0,0,0)}+\delta_{(1,0,0)}+\rho_{(0,0,0)}+\rho_{(1,0,0)}\\&=(x_1+1)(x_2+1)(x_3+1)+x_1(x_2+1)(x_3+1)+1+x_1\\&=x_1+x_2+x_3+x_2x_3\end{aligned}$$

$$\begin{aligned}\gamma_{(1,0)}&=\delta_{(0,1,0)}+\delta_{(1,1,0)}+\rho_{(0,1,0)}+\rho_{(1,1,0)}\\&=(x_1+1)x_2(x_3+1)+x_1x_2(x_3+1)+x_2+x_1x_2\\&=x_1x_2+x_2x_3\end{aligned}$$

$$\begin{aligned}\gamma_{(0,1)}&=\delta_{(0,0,1)}+\delta_{(1,0,1)}+\rho_{(0,0,1)}+\rho_{(1,0,1)}\\&=(x_1+1)(x_2+1)x_3+x_1(x_2+1)x_3+x_3+x_1x_3\\&=x_1x_3+x_2x_3\end{aligned}$$

$$\begin{aligned}\gamma_{(1,1)}&=\delta_{(0,1,1)}+\delta_{(1,1,1)}+\rho_{(0,1,1)}+\rho_{(1,1,1)}\\&=(x_1+1)x_2x_3+x_1x_2x_3+x_2x_3+x_1x_2x_3\\&=x_1x_2x_3.\end{aligned}$$

These 4 functions can be seen to be coincident in the following table

	$\gamma_{(0,0)}$	$\gamma_{(1,0)}$	$\gamma_{(0,1)}$	$\gamma_{(1,1)}$
$(0,0,0)$	0	0	0	0
$(0,1,0)$	1	0	0	0
$(0,0,1)$	1	0	0	0
$(0,1,1)$	1	1	1	0
$(1,0,0)$	1	0	0	0
$(1,1,0)$	0	1	0	0
$(1,0,1)$	0	0	1	0
$(1,1,1)$	0	0	0	1

Theorem 20 *For each $f\in\mathcal{C}_n$ define*

$$f_\delta=\sum_{(u_2,\ldots,u_n)\in GF(2)^{n-1}} f(1,u_2,\ldots,u_n)\ (\delta_{(0,u_2,\ldots,u_n)}+\delta_{(1,u_2,\ldots,u_n)}).$$

and

$$f_\rho=\sum_{(u_2,\ldots,u_n)\in GF(2)^{n-1}} f(1,u_2,\ldots,u_n)\ (\rho_{(0,u_2,\ldots,u_n)}+\rho_{(1,u_2,\ldots,u_n)}).$$

then

$$f=f_\delta+f_\rho=(1+I)*f_\delta=(1+I)*f_\rho.$$

Proof By Theorem 19,

$$f = f_\delta + f_\rho$$

and by Theorem 12,

$$f_\delta * 1 = f_\rho, \quad f_\rho * 1 = f_\delta,$$

therefore,

$$f = (1 + I) * f_\delta = (1 + I) * f_\rho.$$

□

Theorem 21 *A function $f \in \mathcal{B}_n$ is a coincident function if and only if $f = (1+I)*g$ for some function $g \in \mathcal{B}_n$.*

Proof Suppose that $f = (1 + I) * g$. Then, using Theorem 15, we get

$$(1 + I) * f = (1 + I) * (1 + I) * g = 0 * g = 0,$$

so f is a coincident function.
Conversely, suppose that f is a a coincident function. Then by Theorem 20, we have $f = (1 + I) * g$ with $g = f_\delta$. □

5 Conclusion and Future Work

In this paper, we have introduced a new notion, called *Dirichlet product* for boolean functions. We have intensively studied the arithmetical and the algebraic structures of the set of all boolean functions under this Dirichlet product. We have presented the affects of the Dirichlet product on a boolean function and its Möbius transform. We have applied the Dirichlet product to coincident boolean functions and exhibited new properties and characterizations of such functions.
The results presented in this paper on the new notion of Dirichlet product for boolean functions are not exhaustive. They are only the first steps toward further applications of the Dirichlet product, especially in cryptography. We leave it as future work to investigate possible applications of the Dirichlet product to find useful results to compute the algebraic degree of a boolean function and to characterize cryptographic properties such as nonlinearity, balancedness, correlation immunity and algebraic immunity.

References

1. T.M. Apostol, Introduction to Analytic Number Theory, Springer, 1976.
2. C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes, In Yves Crama and Peter L. Hammer (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pages 257–397, Cambridge University Press, 2010.
3. Y. Crama, P.L. Hammer, Boolean Functions, Theory, Algorithms, and Applications, Cambridge University Press, 2010.
4. D.K. Dalai, K.C. Gupta and S. Maitra, Cryptographically significant boolean functions: construction and analysis in terms of algebraic immunity, In INDOCRYPT 2004, pages 92–106, number 3348, Lecture Notes in Computer Science, Springer-Verlag.
5. J. Pieprzyk and X.M. Zhang, Computing Möbius Transforms of Boolean Functions and Characterizing Coincident Boolean functions, *Proceedings of the International Conference on Boolean Functions: Cryptography and Applications 2007.*

6. J. Pieprzyk, H. Wang and X.M. Zhang, Möbius transforms, coincident Boolean functions and non-coincidence property of Boolean functions, *International Journal of Computer Mathematics* **88**(7)(2011), 1398–1416.
7. P. Sarkar and S. Maitra: Construction of Nonlinear Boolean Functions with Important Cryptographic Properties, In EUROCRYPT 2000, number 1807 in Lecture Notes in Computer Science, pages 485–506. Springer Verlag, May 2000.