On affine groups coming from hidden sums

Marco Calderini and Massimiliano Sala
Department of Mathematics, University of Trento, Italy
marco.calderini@unitn.it, maxsalacodes@gmail.com

Abstract. We investigate some differential properties of the affine group, of a vector space $V$ over the binary field, with respect to a new operation $\circ$, which induces a new vector space structure on $V$.

1 Introduction

Most modern block ciphers are built using components whose cryptographic strength is evaluated in terms of the resistance offered to attacks on the whole cipher. In particular, differential properties of Boolean functions are studied for the S-Boxes to thwart differential cryptanalysis ([3,9]).

Little is known on similar properties to avoid trapdoors in the design of the block cipher. In [5] the authors investigate the minimal properties for the S-Boxes (and the mixing layer) of an AES-like cipher (more precisely, a translation-based cipher, or tb cipher) to thwart the trapdoor coming from the imprimitivity action, first noted in [10].

In [8], Li observed that if $V$ is a vector space over a finite field $\mathbb{F}_p$, the symmetric group $\text{Sym}(V)$ will contain many isomorphic copies of the affine group $\text{AGL}(V)$, which are its conjugates in $\text{Sym}(V)$. So there are several structures $(V, \circ)$ of a $\mathbb{F}_p$-vector space on the set $V$, where $(V, \circ)$ is the abelian additive group of the vector space. Each of these structure will yield in general a different copy $\text{AGL}(V, \circ)$ of the affine group within $\text{Sym}(V)$.

So, a trapdoor coming from an alternative vector space structure, which we call hidden sum, can be embed in a cipher, whenever the permutation group generated by the round functions of the cipher is contained in a conjugate of $\text{AGL}(V)$. In [4] the authors provide conditions on the S-Boxes of a tb cipher that avoid attacks coming from hidden sums. This result has been generalized to tb ciphers over any field in [2]. Also, in [1], the author studied such trapdoors, characterizing a new class of vectorial Boolean functions, which they call anti-crooked, able to avoid any hidden sum.
In this paper we investigate some properties of affine groups, of a vector space over the binary field, with respect to a hidden sum $\circ$. In particular, we focus on affine groups which contain the translation group with respect to the usual sum $+$, and affine groups whom translation group is contained in $AGL(V)$. In the last part we provide a toy cipher with a hidden-sum trapdoor and show that it can be thus broken with attacks which are: much faster than brute force, independent of the number of rounds, independent of the key-schedule.

2 Preliminaries

Here we give some notation and some results that we are going to use along the paper. In the following, if not specified, $V$ will be a $n$ dimensional vector space over $\mathbb{F}_2$.

With the symbol $+$ we refer to the usual sum over the vector space $V$, and we denote by $T_+$, $AGL(V,+)$ and $GL(V,+)$, respectively, the translation, affine and linear groups w.r.t. $+$. A translation group is an elementary abelian regular group. For abelian regular subgroups of the affine group in [6] was given a simple description of these in terms of commutative associative algebra that one can impose on the vector space.

We report the principal result shown in [6]. Recall that a (Jacobson) radical ring is a ring $(A, +, \cdot)$ in which every element with respect the operation $x \circ y = x + y + x \cdot y$ (here the circle operation cannot induce a vector space structure over $V$).

**Theorem 1.** Let $\mathbb{F}$ be an arbitrary field, and $(V,+)$ a vector space of arbitrary dimension over $\mathbb{F}$.

There is a one-to-one correspondence between

1. abelian regular subgroups $T$ of $AGL(V,+)$, and
2. commutative, associative $\mathbb{F}$-algebra structures $(V,+,\cdot)$ that one can impose on the vector space structure $(V,+)$, such that the resulting ring is radical.

In this correspondence, isomorphism classes of $\mathbb{F}$-algebras correspond to conjugacy classes under the action of $GL(V,+)$ of abelian regular subgroups of $AGL(V,+)$.

**Remark 1.** From the theorem above we can note that in characteristic 2, algebras corresponding to elementary abelian regular subgroups of $AGL(V,+)$ are exterior algebras or a quotient thereof.
We will denote by $\sigma_a$ the translation in $T_+$ such that $x \mapsto x + a$. We will use $T_0$ and $AGL(V, \circ)$ to denote the translation and affine group corresponding to a sum $\circ$. The operation $\circ$ is a hidden sum, introduced before. Since $T_0$ is regular, for each $a \in V$ there is a unique map $\tau_a \in T_0$ such that $0 \mapsto a$. Thus

$$T_0 = \{\tau_a | a \in V\},$$

in particular $\tau_a$ is the $\circ$-translation $x \mapsto x \circ a$.

With $1_V$ we will denote the identity map of $V$.

Remark 2. If $T_0 \subseteq AGL(V, +) = GL(V, +) \ltimes T_+$, then $\tau_a = \sigma_a \kappa$ for some $\kappa \in GL(V, +)$. We will denote by $\kappa_a$ the map $\kappa$ corresponding to $\tau_a$.

Let $T \subseteq AGL(V, +)$ and define the set

$$U(T) = \{a | \tau = \sigma_a, \tau \in T\}.$$ 

It is easy to check that $U(T)$ is a subspace of $V$, whenever $T$ is a subgroup. If $T = T_0$ for some operation $\circ$, then $U(T_0)$ is not empty for the following lemma.

Lemma 1 ([6]). Let $T_+$ be the group of translation in $AGL(V, +)$ and let $T \subseteq AGL(V, +)$ be a regular subgroup. Then, if $V$ is finite $T_+ \cap T$ is nontrivial.

3 On the differential uniformity of a $\circ$-affine map

The round functions of a translation based block cipher (Definition 3.1 [5]) is composed by a parallel s-Box $\gamma$, a mixing layer $\lambda$ and the translation by the round key $\sigma_k$. The map $\gamma$ must be as non-linear as possible to create confusion in the message. An important notion of "non-linearity" of Boolean functions is the differential uniformity.

In this part we give a lower bound for the differential uniformity of the functions contained in an affine group $AGL(V, \circ)$ for the cases when $T_0 \subseteq AGL(V, +)$ and $T_+ \subseteq AGL(V, \circ)$.

We recall the definition of differential uniformity.

Definition 1. Let $m, n \geq 1$. Let $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^n$, for any $a \in \mathbb{F}_2^m$ and $b \in \mathbb{F}_2^n$ we define

$$\delta_f(a, b) = |\{x \in \mathbb{F}_2^m | f(x + a) + f(x) = b\}|.$$
The differential uniformity of $f$ is
\[ \delta(f) = \max_{a \in F_m^2, b \in F_n^2, a \neq 0} \delta_f(a, b). \]
f is said $\delta$-differential uniform if $\delta = \delta(f)$.

**Lemma 2.** Let $T_o \subseteq AGL(V, +)$ and $\dim(U(T_o)) = k$. Then $f \in AGL(V, \circ)$ is at least $2^k$ differentially uniform.

**Proof.** W.l.o.g. $f(0) = 0$. Let $a \in U(T_o)$, then
\[ f(x + a) + f(x) = [f(x) \circ f(a)] + f(x). \]
So, for all $f(x) \in U(T_o)$ we have
\[ [f(x) \circ f(a)] + f(x) = [f(x) + f(a)] + f(x) = f(a), \]
that implies $|\{x \mid f(x + a) + f(x) = f(a)\}| \geq 2^k$.

When $T_+ \subseteq AGL(V, \circ)$, we can define $U_o(T_+) = \{a | \sigma_a \in T_+ \cap T_o\}$ and it is a vector subspace of $(V, \circ)$. Then we obtain, analogously, the following lemma.

**Lemma 3.** Let $T_+ \subseteq AGL(V, \circ)$ and $\dim(U_o(T_+)) = k$, as subspace of $(V, \circ)$. Then $f \in AGL(V, \circ)$ is at least $2^k$ differentially uniform.

Recalling that given a ring $R$, $r \in R$ is called unipotent if and only if $r - 1$ is nilpotent, we have the following:

**Lemma 4.** Let $T_o \subseteq AGL(V, +)$. Then for each $a \in V$, $\gamma_a$ has order 2 and it is unipotent.

**Proof.** We know that $\tau_a$ has order 2, because $T_o$ is elementary. Then, $\tau_a^2 = 1_V$ implies $\tau_a(a) = 0$, and in particular $\kappa_a(a) = a$. So
\[ x = \tau_a^2(x) = \kappa_a(\kappa_a(x) + a) + a = \kappa_a^2(x) + a + a = \kappa_a^2(x) \quad \text{for all } x \in V. \]
That implies $(\kappa_a - 1_V)^2 = \kappa_a^2 - 1_V = 0$.

**Remark 3.** The lemma above holds in any characteristic $p$, in this case the order of $\kappa_a$ is $p$.

**Remark 4.** If a square matrix is unipotent, it is equivalent to the fact that its characteristic polynomial $P(t)$ is a power of $t - 1$, i.e. it has unique eigenvalue 1.
We recall the following definition.

**Definition 2.** Let $A$ be an $n \times n$ matrix over a field $\mathbb{F}$, with $\lambda \in \mathbb{F}$ along the main diagonal and 1 along the diagonal above it, that is

$$A = \begin{bmatrix}
\lambda & 1 & \cdots & 0 \\
0 & \lambda & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & \cdots & \cdots & \lambda 
\end{bmatrix}.$$ 

Then $A$ is called the $n \times n$ elementary Jordan matrix or Jordan block of size $n$.

**Definition 3.** A matrix $A$ defined over a field $\mathbb{F}$ is said to be in Jordan canonical form if $A$ is block-diagonal where each block is a Jordan block defined over $\mathbb{F}$.

The following theorem is well known (see for instance [2]).

**Theorem 2.** Let $A$ an $n \times n$ matrix over a field $\mathbb{F}$ such that any eigenvalue of $A$ is contained in $\mathbb{F}$, then there exists $J$ defined over $\mathbb{F}$ in Jordan canonical form similar to $A$.

**Lemma 5.** For each $a \in V$, $\kappa_a$ fixes at least $2\lfloor \frac{n-1}{2} \rfloor + 1$ elements of $V$.

**Proof.** From Lemma 4, $\kappa_a$ has a unique eigenvalue equals to 1 $\in \mathbb{F}_2$, then from Theorem 2 there exists a matrix over $\mathbb{F}_2$ in the Jordan form similar to $\kappa_a$. Thus, $\kappa_a = AJA^{-1}$, for some $A, J \in GL(V, +)$ with

$$J = \begin{bmatrix}
1 & \alpha_1 & \cdots & 0 \\
0 & 1 & \alpha_2 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & \cdots & 1 & \alpha_{n-1} \\
0 & \cdots & 1 & 1 
\end{bmatrix} \quad \text{and} \quad J^2 = \begin{bmatrix}
1 & 0 & \alpha_1\alpha_2 & \cdots & 0 \\
0 & 1 & 0 & \alpha_2\alpha_3 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
0 & \cdots & 1 & 0 & \alpha_{n-2}\alpha_{n-1} \\
0 & \cdots & 1 & 0 & 1 \\
0 & \cdots & 1 & 1 & 1 
\end{bmatrix}. $$

where $\alpha_i \in \mathbb{F}_2$ for $1 \leq i \leq n - 1$.

From the fact that $J$ is conjugated to $\kappa_a$ we have $J^2 = 1_V$, and that implies $\alpha_i\alpha_{i+1} = 0$ for all $1 \leq i \leq n - 2$.

Note that if $\alpha_i = 1$ then $\alpha_{i-1}$ and $\alpha_{i+1}$ have to be equal to 0. Thus we have that when $n$ is even at most $\frac{n-1}{2}$ $\alpha_i$’s can be equal to 1 then at least $\frac{n}{2}$ elements of the canonical basis are fixed by $J$. When $n$ is odd we
have at most $\frac{n-1}{2}$ $\alpha_i$'s equal to 1 then at least $\frac{n-1}{2} + 1$ elements of the canonical basis are fixed by $J$. Our claim follows from the fact that $\kappa_a$ is conjugated to $J$.

In terms of algebras we have the following corollary.

**Corollary 1.** Let $T_0 \subseteq AGL(V,+)$, and let $(V,+,\cdot)$ be the associated algebra of Theorem [1]. Then for each $a \in V$, $a \cdot x$ is equal to 0 for at least $\frac{n-1}{2} + 1$ elements of $V$.

**Remark 5.** The bound on the number of elements fixed by $\gamma_a$ given in Lemma [1] is tight. In fact let $(V,+)$ be the exterior algebra over a vector space of dimension three, spanned by $e_1, e_2, e_3$. That is, $V$ has basis $e_1, e_2, e_3, e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge e_3, e_1 \wedge e_2 \wedge e_3$.

We have that $e_1 \cdot x = 0$ for all $x \in E = (e_1, e_1 \wedge e_2, e_1 \wedge e_3, e_1 \wedge e_2 \wedge e_3)$. So, for all $x \in E$

$$x \circ e_1 = x + e_1 + x \cdot e_1 = x + e_1.$$

Vice versa if $x \circ e_1 = x + e_1$ then $x \in E$. The cardinality of $E$ is $2^4$.

**Lemma 6.** Let $T_0 \subseteq AGL(V,+)$ . Then $f \in AGL(V,\circ)$ is at least $2^{\frac{n-1}{2}+1}$ differentially uniform.

**Proof.** W.l.o.g. $f(0) = 0$. From Lemma [1] there exists $a \in U(T_0)$ different from zero. So

$$f(x + a) + f(x) = f(x \circ a) + f(x) = [f(x) \circ f(a)] + f(x) = [f(x) + f(a) + f(a) \cdot f(x)] + f(x)$$

Now, from Corollary [1] we have that $f(a) \cdot f(x) = 0$ for at least $2^{\frac{n-1}{2}+1}$ elements of $V$.

This implies $|\{x | f(x + a) + f(x) = f(a)\}| \geq 2^{\frac{n-1}{2}+1}$.

**Lemma 7.** Let $T_+ \subseteq AGL(V,\circ)$. Then $f \in AGL(V,\circ)$ is at least $2^{\frac{n-1}{2}+1}$ differentially uniform.

**Proof.** Note that Theorem [1], Lemma [1], and Corollary [1] hold also inverting the operation $\circ$ and $+$. Then, there exists $a \in V$ different from zero such that $x + a = x \circ a$ for all $x \in V$. Considering the algebra $(V,\circ,\cdot)$ such that $x + y = x \circ y \circ x \cdot y$ for all $x, y \in V$, we have

$$f(x + a) + f(x) = f(x \circ a) + f(x) = [f(x) \circ f(a) \circ f(0)] + f(x) =$$
\[ \begin{align*}
\{ f(x) \circ f(a) \circ f(0) \} \circ f(x) \circ f(x) \cdot \{ f(x) \circ f(a) \circ f(0) \} \\
\{ f(x) \circ f(a) \circ f(0) \} \circ f(x) \circ f(x) \cdot \{ f(x) \circ f(a) \circ f(0) \}.
\end{align*} \]

From Remark 1 we have \( y^2 = 0 \) for all \( y \in V \), and from Corollary 1 \( f(x) \cdot \{ f(a) \circ f(0) \} = 0 \) for at least \( 2^{\lfloor \frac{n-1}{2} \rfloor}+1 \) elements. Thus \( |\{ x | f(x + a) + f(x) = f(a) \circ f(0) \}| \geq 2^{\lfloor \frac{n-1}{2} \rfloor}+1 \).

So we obtain our main result:

**Theorem 3.** Let \( T_0 \subseteq AGL(V, +) \) \( (T_+ \subseteq AGL(V, \circ) \), respectively). Then \( f \in AGL(V, \circ) \) is at least \( 2^m \) differentially uniform, where \( m = \max\{ \lfloor \frac{n-1}{2} \rfloor + 1, \dim(U(T_0)) \} \) (\( m = \max\{ \lfloor \frac{n-1}{2} \rfloor + 1, \dim(U_\circ(T_+)) \} \), respectively).

### 4 A block cipher with a hidden sum

In this section we give an example, similar to that described in [1], of a translation based block cipher in a small dimension, in which it is possible to embed a hidden-sum trapdoor.

Let \( m = 3, n = 2 \), then \( d = 6 \) and we have the message space \( V = F_2^6 \).

The mixing layer of our toy cipher is given by the matrix

\[
\lambda = \begin{bmatrix}
0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0
\end{bmatrix}
\]

Note that \( \lambda \) is a proper mixing layer (see Definition 3.2 [2]). The bricklayer transformation \( \gamma = (\gamma_1, \gamma_2) \) of our toy cipher is given by two identical S-boxes

\[
\gamma_1 = \gamma_2 = \alpha^4 x^6 + \alpha^3 x^4 + \alpha x^3 + \alpha^3 x^2 + x + \alpha^6
\]

where \( \alpha \) is a primitive element of \( F_2^3 \) such that \( \alpha^3 = \alpha + 1 \).

The S-box \( \gamma_1 \) is 4-differential uniform.

Consider the hidden sum \( \circ \) over \( V_1 = V_2 = (F_2)^3 \) induced by the elementary abelian regular group \( T_0 = \langle \tau_1, \tau_2, \tau_3 \rangle \), where

\[
\begin{align*}
\tau_1(x) &= x \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} + e_1, \\
\tau_2(x) &= x \cdot \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + e_2, \\
\tau_3(x) &= x \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + e_3,
\end{align*}
\]

(1)
with $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ and $e_3 = (0, 0, 1)$. In other words, $\tau_i(x) = x \circ e_i$ for any $1 \leq i \leq 3$.

Obviously $T = T_0 \times T_0$ is an elementary abelian group inducing the hidden sum $(x_1, x_2) \circ'(y_1, y_2) = (x_1 \circ y_1, x_2 \circ y_2)$ on $V = V_1 \times V_2$. By a computer check it results $\langle T_+, \lambda \gamma \rangle \subseteq \AGL(V, \circ')$, and $\circ'$ is a hidden sum for our toy cipher. It remains to verify whether it is possible to use it to attack the toy cipher with an attack that costs less than brute force. We are considering a cipher where the number of rounds is so large to make any classical attack useless (such as differential cryptanalysis) and the key scheduling offer no weakness. Therefore, the hidden sum will actually be essential to break the cipher only if the attack that we build will cost significantly less than 64 encryptions, considering that the key space is $\mathbb{F}_2^6$.

Remark 6. $T_0$ is generated by the translations corresponding to $e_1, e_2$ and $e_3$, which implies that the vectors $e_1, e_2, e_3$ form a basis for $(V_1, \circ)$. Let $x = (x_1, x_2, x_3) \in V_1$, from (1) we can simply write

$$
\tau_1(x) = (x_1 + 1, x_2, x_2 + x_3), \tau_2(x) = (x_1, x_2 + 1, x_1 + x_3), \tau_3(x) = (x_1, x_2, x_3 + 1).
$$

Let us write $x$ as a linear combination of $e_1, e_2$ and $e_3$ w.r.t. to the sum $\circ$, i.e. $x = \lambda_1 e_1 \circ \lambda_2 e_2 \circ \lambda_3 e_3$. We have that $\lambda_1 = x_1, \lambda_2 = x_2$ and $\lambda_3 = \lambda_1 \lambda_2 + x_3$. So

$$
(x_1, x_2, x_3) = x = (\lambda_1, \lambda_2, \lambda_1 \lambda_2 + \lambda_3)
$$

(2)

Thanks to the previous remark we can find the coefficients of a vector $v' = (v, u) \in V$ with respect to $\circ'$ by using the following algorithm separately on the two bricks of $v'$.

Algorithm 1

Input: vector $x \in \mathbb{F}_2^3$

Output: coefficients $\lambda_1$, $\lambda_2$ and $\lambda_3$.

[1] $\lambda_1 \leftarrow x_1$;
[2] $\lambda_2 \leftarrow x_2$;
[3] $\lambda_3 \leftarrow \lambda_1 \lambda_2 + x_3$;

return $\lambda_1, \lambda_2, \lambda_3$.

Let $v' = (v, u) \in V$, we write

$$
v = \lambda_1^v e_1 \circ \lambda_2^v e_2 \circ \lambda_3^v e_3 \quad \text{and} \quad u = \lambda_1^u e_1 \circ \lambda_2^u e_2 \circ \lambda_3^u e_3.
$$

We denote by

$$
[v'] = [\lambda_1^v, \lambda_2^v, \lambda_3^v, \lambda_1^u, \lambda_2^u, \lambda_3^u]
$$
the vector with the coefficients obtained from the bricks of $v'$ using Algorithm 1.

Let $\varphi = \varphi_k$ be the encryption function, with a given unknown session key $k$. We want to mount two attacks by computing the matrix $M$ and the translation vector $t$ defining $\varphi \in AGL(V, o')$, so $t = \varphi(0)$ and $[\varphi(x)] = [x] \cdot M + [t]$.

Assume we can call the encryption oracle. Then $M$ can be computed from the 7 ciphertexts $\varphi(0), \varphi(e'_1), \ldots, \varphi(e'_6)$ (where $e'_1 = (1, 0, 0, 0, 0), \ldots, e'_6 = (0, 0, 0, 0, 1)$), since the $([\varphi(e'_i)] + [t])$'s represent the matrix rows. In other words, we will have

$$[\varphi(v')] = [v'] \cdot M + [t], \quad [\varphi^{-1}(v')] = ([v'] + [t]) \cdot M^{-1},$$

for all $v' \in V$, where the product row by column is the standard scalar product. The knowledge of $M$, $t$ and $M^{-1}$ provides a global deduction (reconstruction), since it becomes trivial to encrypt and decrypt. In fact, to encrypt $v$ it is enough to compute $[v]$, applying $[v] \mapsto [v] \cdot M + [t] = [w]$ and then pass from $[w]$ to the standard representation $w$ via (2). Analogously to decrypt. However, following [1], we have an alternative depending on how we compute $M^{-1}$, resulting in one attack with 7 encryptions and another with 7 encryptions and 7 decryptions. Both are much faster than brute-force searching in the keyspace.

References

1. R. Aragona, M. Calderini, and M. Sala. The role of Boolean functions in hiding sums as trapdoors for some block ciphers, arXiv preprint arXiv:1411.7681 (2014).
2. R. Aragona, A. Caranti, F. Dalla Volta, M. Sala, On the group generated by the round functions of translation based ciphers over arbitrary finite fields, Finite Fields and Their Applications 25 (2014), 293–305.
3. E. Biham, A. Shamir Differential cryptanalysis of DES-like cryptosystems. J. Cryptol 4(1) (1991), 3–72.
4. A. Caranti, F. Dalla Volta, and M. Sala, Abelian regular subgroups of the affine group and radical rings, Publ. Math. Debrecen 69 (2006), no. 3, 297–308.
5. A. Caranti, F. Dalla Volta, and M. Sala, An application of the ONan-Scott theorem to the group generated by the round functions of an AES-like cipher, Designs, Codes and Cryptography 52 (2009), no. 3, 293–301.
6. A. Caranti, F. Dalla Volta, and M. Sala, On some block ciphers and imprimitive groups, AAECC 20 (2009), no. 5-6, 229–350.
7. S. Lang, Linear Algebra. Springer Undergraduate Texts in Mathematics and Technology. Springer, (1987).
8. Cai Heng Li, The finite primitive permutation groups containing an abelian regular subgroup, Proceedings of the London Mathematical Society 87 (2003), no. 03, 725–747.
9. K. Nyberg, *Differentially uniform mappings for cryptography*, Advances in Cryptology, EUROCRYPT ’93, Lecture Notes in Computer Science 765 (1994), 55–64.
10. K. G. Paterson, *Imprimitive permutation groups and trapdoors in iterated block ciphers*, Fast software encryption, LNCS, vol. 1636, Springer, Berlin, (1999), pp. 201–214.