CIRCUIT BASES OF STRONGLY CONNECTED DIGRAPHS

PETRA M. GLEISS

Institute for Theoretical Chemistry and Structural Biology,
University of Vienna, Währingerstrasse 17, A-1090 Vienna, Austria
e-mail: pmg@tbi.univie.ac.at

JOSEF LEYDOLD

Dept. for Applied Statistics and Data Processing
University of Economics and Business Administration
Augasse 2-6, A-1090 Wien, Austria
e-mail: Josef.Leydold@statistik.wu-wien.ac.at

PETER F. STADLER

Institute for Theoretical Chemistry and Structural Biology,
University of Vienna, Währingerstrasse 17, A-1090 Vienna, Austria[1]
The Santa Fe Institute, 1399 Hyde Park Rd, Santa Fe NM 87501, USA
e-mail: studla@tbi.univie.ac.at

Abstract

The cycle space of a strongly connected graph has a basis consisting of directed circuits. The concept of relevant circuits is introduced as a generalization of the relevant cycles in undirected graphs. A polynomial time algorithm for the computation of a minimum weight directed circuit basis is outlined.

Keywords: Directed graphs, cycle space, relevant circuits, minimum length basis.

2000 Mathematics Subject Classification: 05C20 (directed graphs), 05C38 (paths and cycles), 05C85 (graph algorithms).

1. INTRODUCTION

Minimum length bases of the cycle space of undirected graphs have a variety of practical applications. They play a crucial role in chemical "ring perception" [6], structural flexibility analysis [16], electrical networks [5], and error propagation in

[1] Address for correspondence

chemical reaction networks [9]. Brief surveys and extensive references can be found e.g. in [13, 14].
In many cases the network graphs of interest are intrinsically directed. It is natural therefore to ask for a description of the cycle structure in terms of circuits, i.e., cycles that are following the directions of the arcs. This problem is of particular interest for the analysis of the metabolites fluxed through the large metabolic reaction networks of a cell. A central issue in Metabolic Flux Analysis [7], for instance, is the computation of a certain basis of "flux modes" which, in the case of networks of isomerization reactions [1] reduces to the problems of finding circuit bases. The selection of a minimal weight basis can help to reduce the ambiguities of previous methods in this field.
This contribution is organized as follows. In the following (rather lengthy) section we introduce the basic notation and collect a number of basis properties of the cycle spaces of directed graphs. In Section 3 we prove a variant of Berge's theorem stating that any strongly connected digraph has a basis consisting of all double edges and a collection of proper circuits that correspond to a cycle basis of the underlying undirected graph. In Section 4 we introduce the concept of "relevant circuits" and derive their main properties. Section 5 is concerned with necessary conditions for a circuit to be relevant. These are used in the final section for the design of an algorithm that extracts a minimal circuit basis in polynomial time from a relatively small collection of certain short cycles by means of a greedy procedure.

2. PRELIMINARIES

2.1. Basic Notation

A *digraph* $G(V, A)$ consists of a set V of *vertices* and a set A of *arcs* (directed edges). We consider only graphs without self-loops and multiple arcs (unless we explicitly use the term multi-graph), hence A can be regarded as a set of ordered pairs of vertices, $A \subset V \times V$. We write $(x, y) = e \in A$ and call x the initial and y the terminal vertex of e. We refer to both x and y as the end-points of the arc e.
A *chain* in G is an alternating sequence of vertices and arcs

$$\mathbf{c} = (x_0, e_1, x_1, e_2, x_2 \ldots, e_{q-1}, x_{q-1}, e_q, x_q) \tag{1}$$

such that either $e_k = (x_{k-1}, x_k)$ or $e_k = (x_k, x_{k-1})$. In the first case we speak of a *forward arc*, in the second case of a *backward arc*. The vertices x_0 and x_q are the initial and terminal vertex of the chain, respectively.
A chain is *closed* if its initial and terminal vertices coincide. A chain that does not contain the same arc twice is *simple*. A chain is *elementary* if each vertex x appears only once with the possible exception that the initial and terminal vertices may coincide. An elementary chain is of course always simple. The length $l(\mathbf{c})$ of the chain $\mathbf{c}$ is the number q of its arcs. A *cycle* is a closed simple chain. Consequently, every cycle is the arc-disjoint union of a collection of elementary cycles.

A *walk* is a chain in which $e_k = (x_{k-1}, x_k) \in A$ for all k, i.e., in which each arc is transversed in forward direction. A *path* is a simple walk. A *circuit* is a simple closed path. An elementary circuit is a closed elementary path and any circuit is therefore the arc-disjoint union of elementary circuits. A cycle or circuit $\mathbf{c}$ is *proper* if $(x,y) \in \mathbf{c}$ implies $(y,x) \notin \mathbf{c}$. Proper cycles therefore have length $|\mathbf{c}| \geq 3$. A circuit of length 2 will be called a *double edge*.
The *directed distance* $d(x,y)$ between two vertices x and y is the length of the shortest path with initial vertex x and terminal vertex y or $d(x,y) = \infty$ if no path from x to y exists. The directed distance satisfies $d(x,y) = 0 \Longrightarrow x = y$ and the directed triangle inequality $d(x,y) + d(y,z) \leq d(x,z)$, while it is in general not symmetric.
If $G(V,A)$ is a digraph, then $G^\circ(V,A^\circ)$ denotes the underlying undirected graph which is obtained by ignoring the direction of the arcs and identifying double edges. In general we write B° for the set of edges of G° obtained from a set $B \subseteq A$ of arcs by ignoring the direction and removing duplicate edges. A directed graph $G(V,A)$ is *weakly connected* if the undirected graph $G^\circ(V,A^\circ)$ is connected.
A directed graph $G(V,A)$ is *strongly connected* if for all $x,y \in V$ there is a path from x to y and a path from y to x. Furthermore, it is well known that $G(V,A)$ is strongly connected if and only if $G(V,A)$ is weakly connected and each arc is contained in a circuit.
A *cut vertex* in $G(V,A)$ is a vertex x such that deleting x and all arcs incident with x either increases the number of weakly connected components. A graph is 2-connected if it has no cut vertex. A *block* of $G(V,A)$ is a maximal weakly connected induced subgraph of $G(V,A)$ that does not contain a cut vertex. Thus a block is either a 2-connected component (each pair of vertices lies on a common elementary cycle), a pair of vertices connected by an arc, or an isolated vertex. Similarly, a *cut edge* is an edge whose removal disconnects the graph. A graph is 2-edge-connected if it has no cut edge.

2.2. Chains and Their Vectors

Let $\mathbf{c_1} = (x_0, e_1, x_1, \ldots, e_l, x_l)$, $\mathbf{c_2} = (y_0, f_1, y_1, \ldots, f_l, y_l)$, and $x_l = y_0$. Then the concatenation $\mathbf{c_1} * \mathbf{c_2} = (x_0, e_1, x_1, \ldots, e_l, x_l = y_0, f_1, f_1, \ldots, f_l, y_l)$ is again a chain. For simplicity we say that two chains $\mathbf{c_1}$ and $\mathbf{c_2}$ *have no interior vertex in common* if $\mathbf{c_1} \cap \mathbf{c_2} \cap V$ does not contain a non-terminal vertex of either chain.
The following observations are obvious:
(1) Any chain can be regarded as the concatenation of its "individual steps" (x_i, e_{i+1}, x_{i+1}).
(2) The concatenation of two walks $\mathbf{c_1}$ and $\mathbf{c_2}$ is again a walk if and only if the initial vertex of $\mathbf{c_2}$ coincides with the terminal vertex of $\mathbf{c_1}$.
(3) If $\mathbf{c_1}$ and $\mathbf{c_2}$ are simple paths that have no interior vertex in common then their concatenation $\mathbf{c_1} * \mathbf{c_2}$ is again a simple path if the initial vertex of $\mathbf{c_2}$ coincides with the terminal vertex of $\mathbf{c_1}$.
(4) If, in addition, the initial vertex of $\mathbf{c_1}$ and terminal vertex of $\mathbf{c_2}$ coincide then

$\mathbf{c_1} * \mathbf{c_2}$ is a circuit.
Let $\mathbf{c}$ be a simple chain in G. Then we define the arc-indexed vector C (with coordinates $C(e)$, $e \in A$) by

$$C(e) = \begin{cases} +1 & \text{if} \quad e = e_k \in \mathbf{c} \quad \text{and} \quad e_k = (x_{k-1}, x_k) \\ -1 & \text{if} \quad e = e_k \in \mathbf{c} \quad \text{and} \quad e_k = (x_k, x_{k-1}) \\ 0 & \text{if} \quad e \notin \mathbf{c} \end{cases} \tag{2}$$

In other words, $C(e) = +1$ if $e \in \mathbf{c}$ is transversed by $\mathbf{c}$ in forward direction, $C(e) = -1$ if $e \in \mathbf{c}$ is transversed in reverse direction and $C(e) = 0$ if $e \notin \mathbf{c}$. For elementary chains there is a one-to-one correspondence between the vector C and the chain $\mathbf{c}$. This is **not** true in general.
The *support* of a vector $C \in \mathbb{R}^{|A|}$ will be denoted by $\text{supp}(C) = \{e \in A | C(e) \neq 0\}$.
If $\mathbf{c_1}$ and $\mathbf{c_2}$ are arc-disjoint chains and the initial vertex of $\mathbf{c_2}$ coincides with the terminal vertex of $\mathbf{c_1}$ then the vector associated with the concatenation $\mathbf{c_1} * \mathbf{c_2}$ is $C_1 + C_2$. This motivates the definition of the vector C for arbitrary chains $\mathbf{c}$ as the sum of the vectors associated with its individual steps. In other words $C(e)$ is the number of times in which $\mathbf{c}$ transverses $e \in A$ in forward direction minus the number of times in which $\mathbf{c}$ transverses e in backward direction.
In the following we use the convention that a capital letter C is the vector associated with the chain $\mathbf{c}$.

2.3. The Cycle Space of a Digraph

The $|V| \times |A|$ *incidence matrix* $\mathbf{H}$ of the digraph G has the entries $\mathbf{H}_{ex} = +1$ if x is the terminal vertex of the arc e, $\mathbf{H}_{ex} = -1$ if x is the initial vertex of e, and 0 otherwise. The *cycle space* $\mathfrak{C}$ of $G(V, A)$ is the subspace of $\mathbb{R}^{|A|}$ that is generated by the cycles of $G(V, A)$. An important and well-known result, see e.g. [4, sect.II.3], is the following

Proposition 1. $U \in \mathfrak{C} \quad \Longleftrightarrow \quad \mathbf{H}U = 0$

A basis of the cycle space can be constructed as follows: Let T be a spanning forest of G. For each $e \notin T$ there is a unique cycle $\mathbf{c}^e$ in $T \cup \{e\}$. The cycles $\mathbf{c}^e$ are the *fundamental cycles* associated with the spanning forest T. The associated set of vectors $\mathcal{C}_T = \{C^e | e \in A \setminus T\}$ is a basis of the cycle space $\mathfrak{C}$, see e.g. [3, Thm.3.4]. The dimension of the cycle space is therefore

$$\nu(G) = |A| - |V| + \mathrm{c}(G^\circ) \tag{3}$$

where $\mathrm{c}(G^\circ)$ denotes the number connected components of G°, i.e., the number of weak components of G. Note that this is the same construction which is used in undirected graphs. Hence we can expect a close relationship between the cycle space of the digraph G and the underlying undirected graph G°.
From the construction of the basis it follows that $\mathfrak{C}$ has a basis consisting of vectors with coordinates -1, 0, or $+1$.

2.4. Elementary Circuits

From a practical point of view those elements of $\mathfrak{C}$ that follow the directions of the arcs in G are of particular interest. The special role of the circuits is emphasized by the following simple result which will be a useful tool in our proofs:

Lemma 2. *Let* $\mathbf{z}$ *be a closed path in* G*. Then there is a collection* $\{C_i\}$ *of elementary circuits such that* $Z = \sum_i a_i C_i$ *with* $a_i \in \mathbb{N}$*.*

Proof. If each vertex in $\mathbf{z}$ is visited exactly once, then $\mathbf{z}$ is an elementary circuit and there is nothing to show. Otherwise $\mathbf{z}$ contains a vertex x that is visited more than once. Let x be the initial and terminal vertex of $\mathbf{z}$. If x is visited in an intermediate step then $\mathbf{z}$ is a concatenation of two closed paths $\mathbf{z_1}$ and $\mathbf{z_2}$ starting from x, and hence $Z = Z_1 + Z_2$. We consider the two parts independently of each other. After a finite number of such decompositions x occurs only as initial/terminal vertex of each partial closed path $\mathbf{z_i}$. Now let y be the first vertex in $\mathbf{z_i}$ that occurs more than once. We have $\mathbf{z_i} = \mathbf{z_i^1} * \mathbf{z_i^2} * \mathbf{z_i^3}$ where $\mathbf{z_i^1}$ is the path from x to y, $\mathbf{z_i^3}$ is the part of $\mathbf{z_i}$ after the last occurrence of y, and $\mathbf{z_i^2}$ is the closed path between the first and last occurrence of z in $\mathbf{z}$. By construction $\mathbf{z_i^1} * \mathbf{z_i^3}$ is a circuit and $\mathbf{z_i^2}$ is a closed path. This leads to a decomposition of $\mathbf{z}$ into a concatenation of (not necessarily distinct) circuits. Thus the vector Z associated with $\mathbf{z}$ is a sum of circuits with positive integer coefficients. ■

Remark. Using the same arguments it can be shown that each path can be written as a concatenation of elementary paths (and circuits). Furthermore, the non-closed paths can be concatenated to yield a single elementary non-closed path.

It is natural hence to consider the *non-negative cone* of the cycle space, $\mathbb{K} = \{X \in \mathfrak{C} | X_k \geq 0\}$. A vector $U \in \mathbb{K}$ is *extremal* if

$$U = \sum_k \lambda_k X_k,\ X_k \in \mathbb{K} \text{ and } \lambda_k > 0 \quad \text{implies} \quad X_k = \xi_k U \text{ with } \xi_k > 0\,, \tag{4}$$

i.e., if U cannot be represented as a positive linear combination of other vectors from the cone $\mathbb{K}$.

Lemma 3. *If* U *is extremal in* $\mathbb{K}$ *and* $X \in \mathbb{K}$ *such that* $X \neq 0$ *and* $\operatorname{supp}(X) \subseteq \operatorname{supp}(U)$*; then* $X = \mu U$ *for some* $\mu > 0$*, i.e. there are no distinct extremal elements with the same support.*

Proof. Let $\lambda = \min\{U(e)/X(e) | e \in \operatorname{supp}(X)\}$. Then $\lambda X(e) \leq U(e)$ with equality for at least one $e \in \operatorname{supp}(X)$. Consider $W = U - \lambda X$. We have $W \in \mathbb{K}$ since $W(e) \geq 0$ for all $e \in A$. Thus we can write $U = W + \lambda X$. Hence $W = 0$ by the extremality of U and consequently $U = \lambda X$, with $\lambda > 0$ and thus $X = \frac{1}{\lambda} U$. ■

The following proposition is well known, see e.g. [20, 8]. We include the simple argument here to make this contribution self-contained.

Proposition 4. *The elementary circuits of G are exactly the extremal vectors of the cone $\mathbb{K}$.*

Proof. It follows immediately from Prop. 1 that the subgraph G^X of G with edge set $\text{supp}(X)$ for any $X \in \mathbb{K}$ has neither a sink (vertex with out-degree 0) nor a source (vertex with in-degree 0). Therefore G^X contains a circuit. Consequently, no proper subset of an elementary circuit can be the support of a vector in $\mathbb{K}$, i.e., every elementary circuit is an extremal vector of $\mathbb{K}$.
To see the converse, suppose $X \in \mathbb{K}$ is extremal. Let C be an elementary circuit contained in $\text{supp}(X)$, $\mu = \min_{e \in C} X(e)$, and $X' = X - \mu C$. We have $X'(e) \geq 0$ and hence $X' \in \mathbb{K}$. Since X is extremal we must have $X' = 0$ and thus $\text{supp}(X)$ must be an elementary circuit. ■

Theorem 5. *Let $X \in \mathbb{K}$ with integer coordinates. Then there is a collection $\mathcal{Q}$ of (vectors associated with) elementary circuits such that*

$$X = \sum_{C \in \mathcal{Q}} a(C)\, C \quad \textit{with} \quad a(C) \in \mathbb{N} \quad \textit{and} \quad \text{supp}(C) \subseteq \text{supp}(X) \tag{5}$$

Proof. If X is extremal there is nothing to show. Otherwise, let C be (a vector of) an elementary circuit with $\text{supp}(C) \subset \text{supp}(X)$. Set $q = \min\{X(e) | e \in \text{supp}(C)\} \geq 1$ and $X' = X - qC$. We have $\mathbf{H}X' = 0$ by linearity, $X'(e) \geq 0$, i.e., $X' \in \mathbb{K}$, $q \in \mathbb{N}$, and $\text{supp}(X') \subseteq \text{supp}(X)$. Furthermore, $X'(e) = 0$ for at least one $e \in \text{supp}(X)$. Hence we obtain the desired decomposition by repeating the argument a finite number of times. ■

In the following sections we will be concerned with bases of the cycle space $\mathfrak{C}$. In order to simplify the language we will simply say "a circuit C" instead of "a vector C associated with a circuit $\mathbf{c}$". Strictly speaking, this amounts to considering equivalence classes of paths and circuits that yield the same vector representation.

3. CIRCUIT BASES

Definition 1. A *circuit basis* is a basis of the cycle space $\mathfrak{C}$ of $G(V, A)$ consisting exclusively of elementary circuits. A *cycle basis* is a basis of the cycle space $\mathfrak{C}$ of $G(V, A)$ consisting exclusively of elementary cycles.

Lemma 2 raises the question under which conditions the circuits generate the cycle space. This question was essentially answered by Berge [3]:

Proposition 6. *[3] A strongly connected digraph $G(V, A)$ has a circuit basis.*

The converse of Prop. 6 is easily obtained:

Theorem 7. *A digraph $G(V,A)$ has a circuit basis if and only if each block is either strongly connected or a single arc.*

Proof. The cycle space of $G(V,A)$ is the direct sum of the blocks of G. Thus $G(V,A)$ has a circuit basis if each block has a circuit basis or an empty cycle space. The only blocks with empty cycle space are isolated vertices and pairs of vertices that are connected by a single arc. Thus consider a 2-connected block $G(V,A)$ that is not strongly connected. Then there is a cut Q partitioning V into two non-empty subsets V' and V'' such that all arcs in Q point from V' to V''. Choose an arc $e \in Q$; by 2-connectedness e is contained in a cycle C. This cycle passes from V' to V'' and back hence it cannot be a circuit. Thus $\mathfrak{C}$ does not have a circuit basis since e is contained in a cycle but not in a circuit. ■

In other words, $G(V,A)$ has a circuit basis if and only if its strongly connected components are linked together in a tree-like fashion by individual arcs or sequences of individual arcs. Because of this simple structure we shall restrict ourselves to 2-connected digraphs from here on.
Double edges, i.e., circuits of length 2, play a special role, since they are a major difference between graphs and digraphs. For instance, the cyclomatic number of the underlying undirected graph is

$$\nu(G^\circ) = |A^\circ| - |V| + \mathrm{c}(G^\circ) = |A| - d^*(G) - |V| + \mathrm{c}(G^\circ) = \nu(G) - d^*(G) \qquad (6)$$

where $d^*(G)$ denotes the number of double edges in G.

Lemma 8. *Let $\mathcal{B}^\circ$ be a cycle basis of the undirected graph G°, and let $\mathcal{D}(G)$ be the set of double edges of G. Then $\mathcal{B} = \mathcal{B}^\circ \cup \mathcal{D}(G)$ is a cycle basis of G with length*

$$\ell(\mathcal{B}) = \ell(\mathcal{B}^\circ) + 2|\mathcal{D}| \qquad (7)$$

Proof. The cycles in $\mathcal{B}^\circ$ are of course independent cycles of G. At each double edge, we may choose one of the arcs to be part of the $\mathcal{B}^\circ$-cycles that contains the double edge. This shows that the double edges in $\mathcal{D}$ are indeed independent of the set of $\mathcal{B}^\circ$-cycles. Equ.(6) hence implies that $\mathcal{B}$ is a cycle basis of G. Equ.(7) now follows immediately. ■

The following proposition shows that double edges are in a sense superfluous:

Proposition 9. *[18] If $G(V,A)$ is strongly 2-edge-connected then one can obtain a strongly connected graph $G^*(V,A^*)$ by removing one of the two arcs of each double edge.*

The main result of this section is a variant of Prop. 6 (Berge's theorem).

Theorem 10. *A strongly connected digraph $G(V,A)$ has a circuit basis consisting of the $d^*(G)$ double edges and $\nu(G^\circ)$ proper elementary circuits.*

Proof. We follow the construction of a cycle basis consisting of circuits described in [3, Thm.3.9] and [10] with slight modifications. Clearly the theorem is correct for $|V| \leq 2$. Suppose the assertion is correct for all graphs with $k < |V|$ vertices. Let $\mathbf{c}^* = (x_0, e_1, x_1, \ldots, x_{h-1}, e_h, x_0)$ be a shortest circuit in G, $h \geq 2$. Such a circuit exists as a consequence of strong connectedness. Clearly, it is elementary. In particular, if G contains double edges, we choose one of them.
Next we construct a multi-digraph G' by replacing the circuit $\mathbf{c}^*$ (with vertex set W) by a single vertex x^* and by replacing each arc (y,z), $y \neq W$, $z \in W$ by an arc from y to x^* and each arc (z,y) by an arc from x^* to y. In particular, any double edge in G (except $\mathbf{c}^*$ itself if it is a double edge) becomes a double edge in G'. This contraction step may lead to multiple parallel arcs incident with x^*. The resulting multi-digraph has $|A| - h$ edges and $|V| - |W| + 1 = |V| - h + 1$ vertices, i.e., $\nu(G') = \nu(G) - 1$.
Instead of iterating this construction immediately as in the original proofs of Prop. 6 [3, 10] we first take care of the multiple arcs in G'. To this end we select one of the multiple arcs, say g; if one of them is part of a double edge of G it gets selected first. Let C_g be a shortest circuit through g in G'; note that if g was part of a double edge in G, then C_g is just this double edge. We store C_g in a set $\mathcal{C}^*$ and delete the arc g from G', obtaining a multi-digraph G''. We repeat this procedure until, after removing q arcs, there are no further parallel arcs and we are left with a digraph G^*. All double edges that have become part of multiple arcs in G' are now contained in $\mathcal{C}^*$, all other double edges are passed on as double edges to G^*.
Thus G^* has $|V| - h + 1$ vertices and $|A| - h - q$ edges, i.e., its cyclomatic number is $\nu(G^*) = \nu(G) - 1 - q$. Clearly the circuits in $\mathcal{C}^*$, which are elementary by construction, are independent since each uniquely contains one of the q removed parallel arcs. Consequently, the union $\mathcal{C}^{**}$ of $\mathcal{C}^*$ with any cycle basis of G^* consists of $\nu(G) - 1$ independent cycles and hence is a basis of the circuit space of the multi-digraph G'. The induction hypothesis assumes that there is a circuit basis of G^*, hence $\mathcal{C}^{**}$ can be chosen such that it is a circuit basis of G'.
Now recall that each edge incident with x^* in G' corresponds to an edge incident with a particular vertex $x_k \in W$. Thus each circuit $\mathbf{c} \in \mathcal{C}^{**}$ is either an elementary circuit in G if it does not contain x^* or it can be lifted to a unique circuit $\hat{\mathbf{c}}$ in G by replacing x^* with the vertices at which $\mathbf{c}$ "enters" and "leaves" $\mathbf{c}^*$ and the unique path within $\mathbf{c}^*$ that connects these two vertices. The set

$$\mathcal{C} = \{\hat{\mathbf{c}} | \mathbf{c} \in \mathcal{C}^{**}\} \cup \{\mathbf{c}^*\} \tag{8}$$

contains $\nu(G') + 1 = \nu(G)$ elementary circuits, among which are all $d^*(G)$ double edges. Finally, consider the equation

$$\sum_{\mathbf{c} \in \mathcal{C}^{**}} a_{\mathbf{c}} \hat{C} + a^* C^* = 0\,. \tag{9}$$

First we note that $C^*(e) = 0$ for all $e \in A \setminus \mathbf{c}^*$. Thus, restricting equ.(9) to the arcs in $A \setminus \mathbf{c}^*$ and using that the arcs $\mathbf{c} \in \mathcal{C}^{**}$ are linearly independent, we obtain $a_{\mathbf{c}} = 0$

for all $\mathbf{c} \in \mathcal{C}^{**}$. Therefore $a^* C^* = 0$, and $\mathcal{C}$ is indeed a set of $\nu(G)$ independent circuits of G. ■

As a consequence of Thm. 7 we will restrict our attention in the remainder of this contribution to strongly connected digraphs.

4. Minimum Circuit Bases and Relevant Circuits

For a vector $Z \in \mathfrak{C}$ with integer coordinates we set

$$|Z| = \sum_{e \in A} |Z(e)| \tag{10}$$

It follows from Thm. 5 that for all $Z \in \mathbb{K}$ with integer coordinates there is a set $\mathcal{Q}$ of elementary circuits such that $|Z| = \sum_{C \in \mathcal{Q}} a(C)|C|$ with $a(C) \in \mathbb{N}$. Furthermore, we have $|Z| \geq |\text{supp}(Z)|$, with equality if and only if $Z(e) \in \{+1, 0, -1\}$, i.e., if and only if Z is an edge-disjoint union of cycles. In particular, the elementary circuits are the minimal integer-valued elements of $\mathbb{K}$.

Lemma 11. *Let $\mathcal{B} \subset \mathbb{K}$ be a basis of $\mathfrak{C}$ with integer coordinates. If $\mathcal{B}$ has minimum length then it consists exclusively of elementary circuits.*

Proof. Suppose Z is not an elementary circuit. Then it can be written in the form (5), and $|Z| > |C|$ for all $C \in \mathcal{Q}$. Furthermore, we can replace Z by one of the elementary circuits in $\mathcal{Q}$. The resulting basis is strictly shorter than $\mathcal{B}$ and still contains only vectors from the positive cone $\mathbb{K}$ with integer coordinates. Thus $\mathcal{B}$ was not minimal. ■

Bases of the circuit space with minimum total length

$$\ell(\mathcal{B}) = \sum_{C \in \mathcal{B}} |C| \tag{11}$$

consisting of integer-valued vectors, $C(e) \in \mathbb{Z}$, are of particular interest.

Definition 2. A *minimum cycle (circuit) basis* is a cycle (circuit) basis with minimal length.

Theorem 12. *Let G be strongly connected and let C be a shortest circuit through an arc $e \in A$. Then there is a minimum circuit basis that contains C. If C is the unique shortest circuit through e, then every minimal circuit basis contains C.*

Proof. Suppose $\mathcal{B}$ is a minimal circuit basis, and let $e \in A$. Set $\mathcal{B}^e = \{C \in \mathcal{B} | e \in C\}$ and $\mathcal{B}^* = \mathcal{B} \setminus \mathcal{B}^e$. Suppose C is a shortest circuit containing e, $C \notin \mathcal{B}^e$. Since $\mathcal{B}^* \cup \{C\}$ is obviously an independent set, there exists a circuit $C' \in \mathcal{B}^e$ such that $\mathcal{B}' = \mathcal{B} \cup \{C\} \setminus \{C'\}$ is a circuit basis with length $\ell(\mathcal{B}') = \ell(\mathcal{B}) + |C| - |C'| \leq \ell(\mathcal{B})$, since we have assumed $|C| \leq |C'|$. If C is the unique shortest cycle through e we have $|C| < |C'|$, and hence $\ell(\mathcal{B}') < \ell(\mathcal{B})$, contradicting the minimality of $\mathcal{B}$. Thus $C \in \mathcal{B}$ for every minimal circuit basis. ■

The argument used for the proof of Thm. 12 is the same as in the case of minimal cycle bases of undirected graphs [21].

Corollary 13. *Every minimal circuit basis $\mathcal{B}$ of a strongly connected digraph contains the set $\mathcal{D}$ of double edges.*

Proof. If $e \in A$ is part of a double edge, then the double edge $D = \{e, e'\}$ is the unique shortest circuit containing e. By Thm. 12 D is an element of every minimal circuit basis. ■

It is sometimes useful to consider undirected graphs as symmetric digraphs, i.e., as digraphs in which $(x, y) \in A$ implies (y, x) in A. The following result shows that minimum cycle bases of undirected graphs and minimum circuit bases of symmetric digraphs are essentially the same.

Theorem 14. *Let G be a symmetric digraph. Then every minimum circuit basis consists of the set $\mathcal{D}$ of double edges and a set $\mathcal{B}$ of circuits such that $\mathcal{B}^\circ = \{C^\circ | C \in \mathcal{B}\}$ is a minimum cycle basis of the undirected graph G°.*

Proof. It follows from equ.(6) that a minimum circuit basis of G cannot be shorter than $2|\mathcal{D}| + L$, where L is the length of a minimum cycle basis of G°. Conversely, if $\mathcal{B}$ is a minimum circuit basis, then $\mathcal{B} \setminus \mathcal{D}$ is a set of $\nu(G^\circ)$ independent proper cycles and corresponds to a cycle basis of G° with the same length.
Now assume that G is symmetric, i.e., $2|\mathcal{D}| = |A|$. We will show that every minimum cycle basis $\mathcal{B}^\circ$ of G° can be lifted and extended to a circuit basis of G with length $L + |A|$, which, as a consequence of the previous paragraph must then be a minimum circuit basis. To this end we identify each edge e of G° with one of the two arcs of G forming the corresponding double edge. This amounts to lifting $\mathcal{B}^\circ$ to the digraph G. Clearly, $\mathcal{B}^* = \mathcal{B}^\circ \cup \mathcal{D}$ is a basis of the cycle space with the minimum possible length. However, the cycles $C \in \mathcal{B}^\circ$ will in general not be circuits.
For each "negative" edge e, $C(e) = -1$, of a basis cycle C, there is a double edge $D = \{e, e'\} \in \mathcal{D}$ such that either $C' = C + D$ or $C' = C - D$ is a cycle that coincides with C except for e, which is replaced by the forward edge e', $C'(e') = +1$. Clearly, C and C' have the same length and belong to the same cycle C° of the undirected graph G°. Since D is contained in $\mathcal{B}^*$, $\mathcal{B}^{**} = \mathcal{B}^* \cup \{C'\} \setminus \{C\}$ is a basis of the cycle space with the same length. Repeating this argument for all negative edges in C replaces the basis cycle C with a basis circuit C^+ of the same length. Note that C and C^+ by construction belong to the same cycle C° of G°. We finally obtain a circuit basis of G with length $L + |A|$. ■

The set of circuits of $G(V, A)$ forms a matroid. A basis of the cycle space with minimum weight can therefore be obtained by means of the greedy algorithm [17] from the set of all circuits.

Definition 3. Let $(\mathcal{Q},\mathfrak{J})$ be a matroid on $\mathcal{Q}$ with the set $\mathfrak{J}$ of independent sets and let $|\,.\,| : \mathcal{Q} \to \mathbb{R}^+$ be a non-negative weight function on $\mathcal{Q}$. Then $A \in \mathcal{Q}$ is $|\,.\,|$-relevant if there is a minimum weight basis $\mathcal{B}$ of $(\mathcal{Q},\mathfrak{J})$ containing A.

Definition 3 is the obvious generalization of Vismara's relevant cycles of a graph [23, 24].

Theorem 15. *Let $(\mathcal{Q},\mathfrak{J})$ be a matroid with a non-negative weight function $|\,.\,|$ and $C \in \mathcal{Q}$. Furthermore, let*

$$\mathfrak{J}_< = \{\mathcal{W} \in \mathfrak{J} \big| |W| < |C| \text{ for all } W \in \mathcal{W}\}$$

Then C is $|\,.\,|$-relevant if and only if $\mathcal{W} \cup \{C\} \in \mathfrak{J}$ for all $\mathcal{W} \in \mathcal{J}_<$.

Proof. Let A be $|\,.\,|$-relevant. Thus there is a minimum weight basis $\mathcal{B}$ with $A \in \mathcal{B}$. Let $\mathcal{W}$ be an independent set with $|A'| < |A|$ for all $A' \in \mathcal{W}$. Now suppose $\mathcal{W} \cup \{A\}$ is dependent. Then there is an element $A'' \in \mathcal{W}$ such that $\mathcal{B}' = (\mathcal{B} \setminus \{A\}) \cup \{A''\}$ is again a basis. We have $\ell(\mathcal{B}') < \ell(\mathcal{B})$ contradicting the assumption that $\mathcal{B}$ has minimum weight. Hence $\mathcal{W} \cup \{A\}$ must be independent.
The converse implication follows directly from the applicability of the greedy algorithm. ∎

As an immediate consequence of Thm. 5 we may specialize Thm. 15 for circuits in the following form:

Corollary 16. *A circuit is relevant if and only if it cannot be written as linear combination of shorter circuits.*

We can now use Vismara's approach [24] to extract the set $\mathcal{R}_{|\,.\,|}$ of $|\,.\,|$-relevant matroid elements by means of the modified greedy algorithm 1 from $\mathcal{Q}$.

Lemma 17. *Algorithm 1,* R-Greedy*, works.*

Proof. For a set $\mathcal{Z}$ let us write $\mathcal{Z}_{<w} = \{A \in \mathcal{Z} \big| |A| < w\}$, and let $\mathcal{B}$ be a minimum weight basis. Then A is a relevant element if and only if $\mathcal{B}_{<|A|} \cup \{A\} \in \mathfrak{J}$, since we can order $\mathcal{Q}$ such that A is the first element with weight $|A|$ in the prescribed order. ∎

Algorithms for listing all circuits of a digraph are available, see e.g. [15, 19]. The number of circuits in a digraph $G(V, A)$ may be very large, however. The straightforward application of the greedy algorithm or of Algorithm 1 to the set of all circuits will therefore not be feasible in most cases. In the case of undirected graphs one can drastically reduce the initial set of cycles [2, 14, 24]. In the following section we consider similar constructions for circuits in digraphs. The main difference is that in the undirected graph one can work over $GF(2)$ and explicitly use the vector addition of cycles. Here we have the additional problem that the sum of circuits is in general not a circuit.

Algorithm 1 R-Greedy [24]

Input: $(\mathcal{Q}, \mathfrak{J})$, $|\,.\,|$

Output: $\mathcal{R}$ /* Set of $|\,.\,|$-relevant elements. */

Sort $\mathcal{Q}$ by weight: $\{A_1, A_2, \ldots, A_m\}$; /* A_1 with minimal weight. */
Add A_0, A_{m+1} with $|A_0| = 0$ and $|A_{m+1}| = \infty$;
$\mathcal{B}_< \leftarrow \emptyset$; $\mathcal{B}_= \leftarrow \emptyset$; $\mathcal{R}_= \leftarrow \emptyset$; $\mathcal{R} \leftarrow \emptyset$;
for $k = 1$ to $m + 1$ **do**
  if $|A_k| > |A_{k-1}|$ **then**
    $\mathcal{R} \leftarrow \mathcal{R} \cup \mathcal{R}_=$; $\mathcal{B}_< \leftarrow \mathcal{B}_< \cup \mathcal{B}_=$;
    $\mathcal{R}_= \leftarrow \{A_k\}$; $\mathcal{B}_= \leftarrow \{A_k\}$;
  else
    if $\{A_k\} \cup \mathcal{B}_< \in \mathfrak{J}$ **then**
      $\mathcal{R}_= \leftarrow \mathcal{R}_= \cup \{A_k\}$;
    if $\{A_k\} \cup \mathcal{B}_< \cup \mathcal{B}_= \in \mathfrak{J}$ **then**
      $\mathcal{B}_= \leftarrow \mathcal{B}_= \cup \{A_k\}$;

In practice the test for linear independence $\mathcal{X} \in \mathfrak{J}$ is performed e.g. by Gauss-Jordan elimination. In order to reduce the computational effort we therefore compute a minimal basis $\mathcal{B}$ "on the fly".

5. SHORT CIRCUITS

Definition 4. A circuit C is *isometric* if for any two of its vertices x and y it contains a shortest path from x to y *and* a shortest path from y to x.
A circuit C is *short* if for any two of its vertices x and y it contains a shortest path from x to y *or* a shortest path from y to x.
A circuit C is *strictly arc-short* if for each x in C there is an arc $e^x = (v, w)$ such that $C = P[w, x] + P[x, v] + (v, w)$ where $P[w, x]$ and $P[x, v]$ are shortest paths.
A circuit C is *arc-short* if C contains a vertex x and an arc $e = (v, w)$ such that $C = P[w, x] + P[x, v] + (v, w)$ where $P[w, x]$ and $P[x, v]$ are shortest paths.

Lemma 18. *Every isometric circuit is short. A circuit C is short if and only if it is strictly arc-short. Every short circuit is arc-short.*

Proof. It follows directly from the definition that an isometric circuit is short. For two distinct vertices $x \neq y$ in C, we denote the path from x to y in C by $C[x, y]$. Furthermore, we write $S[x, y]$ for a path from x to y in G that is shorter than $C[x, y]$ provided such a di-path exists. We call $S[x, y]$ a shortcut from x to y. In this case $S[x, y] \cup C[y, x]$ is a closed path and hence a linear combination of shorter circuits.
Suppose C is short. First we note that in this case there cannot be a vertex x in C such that there are two vertices y, y' in C and shortcuts $S[x, y]$ and $S[y', x]$. Hence we have to consider three cases for each vertex x in C:

(i) There is no shortcut to or from x in C. Then we may choose any arc $e = (u, v)$ in C and see that $C[x, u]$ and $C[v, x]$ are shortest paths.
(ii) There is a shortcut from x to some y in C, see the l.h.s. of Fig. 1. Then there is also a shortcut $S[x, w]$ from x to every vertex w in $C[y, x]$ (via $S[x, y]$). We can choose y such that it is maximal in the sense that there is no shortcut $S[x, w]$ for all $w \neq y$ in $C[x, y]$. Necessarily there is an arc $e = (z, y) \in C[x, y]$. Hence $C[x, z]$ is a shortest path. Since C is short $C[y, x]$ must be a shortest path and the proposition follows.
(iii) There is a shortcut from some y in C to x, see the r.h.s. of Fig. 1. This implies that there is a shortcut $S[w, x]$ for all w in $C[x, y]$. Again we choose y maximal in the sense that there is no shortcut from w to x for all $w \neq y$ in $C[y, x]$. Then there is an arc $e = (y, z) \in C[y, x]$. If $C[x, y]$ is not a shortest path then there is a shortcut $S[x, y]$ and C is not short.

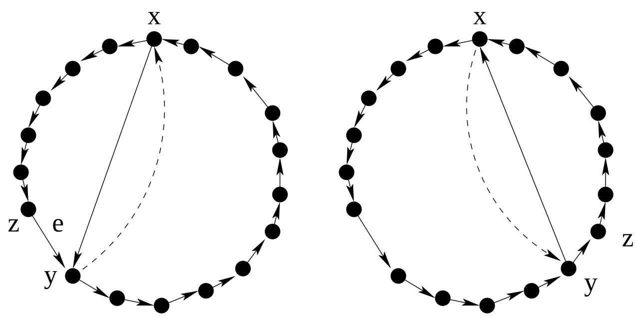

Figure 1: Cases (ii) and (iii) of Lemma 18. For details see text.

Conversely, suppose C is not short. We show that C is not strictly arc-short. If C is not short then there are two vertices $x \neq y$ in C such that there are two shortcuts $S[x, y]$ and $S[y, x]$. Now suppose there is an arc $(u, v) \in C$ such that there is neither a shortcut $S[x, u]$ nor a shortcut $S[v, x]$. Since there is a shortcut $S[x, y]$ there are also shortcuts $S[x, y']$ for all y' in $C[y, x]$. Thus u cannot lie in $C[y, x]$. Similarly, there is a shortcut $S[y', x]$ for all y' in $C[x, y]$ and hence v cannot be in $C[x, y]$. Hence u must be in $C[x, y] \setminus \{x, y\}$ and v must be in $C[y, x] \setminus \{x, y\}$. Thus there cannot be an arc from u to v in C.
Finally, a strictly arc-short circuit is trivially arc-short. ■

In undirected graphs, where a path from x to y is a path from y to x, a short cycle is trivially isometric. In directed graphs, a circuit is *isometric* if for all pairs of vertices $x, y \in \mathbf{c}$ the distance along the circuit equals the directed distance in G, i.e., $d_{\mathbf{c}}(x, y) = d(x, y)$. In general, short circuits therefore are not isometric, as the graph G_1 in Fig. 2 shows.
We observe that a double edge is obviously isometric. However, not all strongly connected digraphs have cycle bases consisting of isometric circuits. The graph G_2

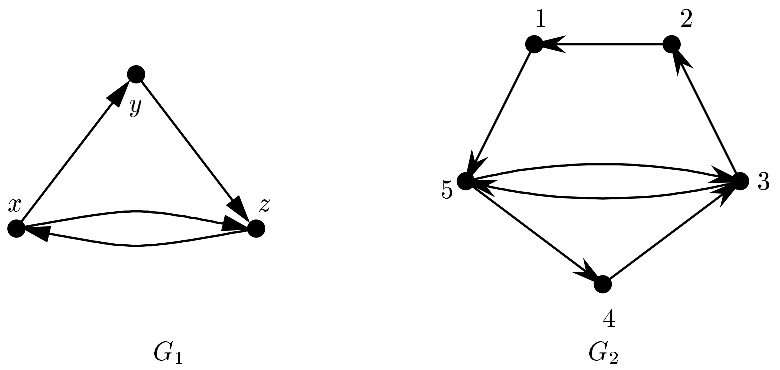

Figure 2: The graph G_1 has $\nu = 4-3+1 = 2$. The only circuits are the double edge $D = (x, z)$ and the triangle $T = (x, y, z)$ which is not isometric since $d_T(x, z) = 2 < d(x, z) = 1$. However, T is short, since for any two points, a shortest path in one of the two directions runs along T.
The pentagon in G_2 is not short since there are shortcuts $S[3, 5]$ and $S[5, 3]$. It is arc-short, however, because it consists of the arc $(2, 1)$ and the shortest paths $P[1, 4]$ and $P[4, 2]$.

in Fig. 2 serves a counter-example. Arc-short circuits are useful because they can be constructed rather easily. In analogy to the undirected case only short circuits can be part of a minimum circuit basis.

Theorem 19. *If C is relevant then C is short.*

Proof. Suppose C is contained in a minimum circuit basis and it is not short. Then there are two vertices x and y in C such that C contains neither a shortest path $S[x, y]$ from x to y nor a shortest path $S[y, x]$ from y to x. As above, we write $C[x, y]$ and $C[y, x]$ for the paths from y to x and from x to y along C, respectively. Note that $C^1 = C[x, y] + S[y, x]$, $C^2 = S[x, y] + C[y, x]$, and $C^3 = S[x, y] + S[y, x]$ correspond to closed paths in G and by Lemma 2 each of them can be written as a (positive) linear combination of circuits none of which is longer than C^1, C^2, or C^3, respectively. By assumption we have $|C^i| < |C|$, for $i = 1, 2, 3$. From

$$C = C[x, y] + C[y, x] = C^1 + C^2 - C^3$$

we find that C itself can be written as a linear combination of circuits, all of which are strictly shorter than C itself. Thus C is not relevant by Cor. 16, a contradiction. ∎

Theorem 19 is the direct generalization of the analogous result for undirected graphs [11, 14]. The notion of short circuits, however, appears to be weaker in directed graphs than in their undirected counterparts.

6. A Polynomial Time Algorithm for Minimum Circuit Bases

The discussion in the previous section suggests a simple generalization of Horton's algorithm to minimal circuit bases: (1) Find a shortest path $S[x,y]$ between any two vertices x and y; (2) from each $(x,y) \in A$ and $z \in V$ construct an arc-short circuit $C_{xy,z} = (x,y) + S[y,z] + S[z,x]$ and (3) use the greedy algorithm to extract a basis. This procedure works in the undirected case since one can show that *any* choice of a — usually not unique — shortest path $S[x,y]$ will work [14]. The ideas behind the proof of this result, however, are not applicable to paths in digraphs.

We may, however, exploit a trick used e.g. in [12], namely perturbing the arc weights by a small amount in such a way that no distinct subsets of A have the same weight. Then the greedy algorithm can select the unique minimal weight basis from the set of arc-short cycles that can be constructed unambiguously because the shortest path $S[x,y]$ from x to y is unique. If the perturbation of the weights is small enough, then the weight of a basis $\mathcal{B}$ is arbitrarily close to the unperturbed weight. Therefore the unique minimum weight basis of the perturbed version is indeed one of the minimum weight bases of the unperturbed problem.

It is easy to see that a perturbation with the desired properties indeed exists. For instance, we label the arcs in some prescribed order by the positive integers $\#e = 1, \ldots, |A|$ and then set $w(e) = 1 + \varepsilon 3^{-\#e}$, $0 < \varepsilon \ll 1$. For $\varepsilon < (|A||V|)^{-1}$ the difference between the length $\ell(\mathcal{B})$ and the perturbed length $w(\mathcal{B})$ of the basis $\mathcal{B}$ is smaller than 1, hence the minimum weight basis is indeed a minimum circuit basis.

In practice, the weighting scheme is of course numerically problematic. It can, however, be replaced by a suitable lexicographic ordering of the arc sets.

Theorem 20. *The complexity of computing a minimum circuit basis is at most* $\mathcal{O}(\nu(G)|A|^2|V|)$.

Proof. The collection of all shortest paths $S[x,y]$ can be obtained e.g. by a variant of Dijkstra's or Floyd's algorithm in $\mathcal{O}(|V|^3)$ operations, see e.g. [22]. There are at most $\mathcal{O}(|A||V|)$ arc-short circuits. Testing whether a candidate circuit is elementary can be done in $\mathcal{O}(|V|)$ steps, this stage requires $\mathcal{O}(|A||V|^2)$ operations. Since $|A| \geq |V|$ this is less expensive than $\mathcal{O}(|A|^2|V|)$. The greedy algorithm requires at most $\mathcal{O}(|A||V|)$ tests for linear independence: each arc-short circuit must be tested against a partial basis which contains at most $\mathcal{O}(\nu(G))$ circuits. Gauss elimination thus requires $\mathcal{O}(|A|\nu(G))$ operations for each arc-short circuit. Hence the worst case requirement is $\mathcal{O}(|A|^2|V|\nu(G))$. ■

As in the case of minimum cycle bases of undirected graphs [14] we expect that the algorithm performs much better for most graphs than the worst case estimate of Thm. 20 suggests.

Acknowledgement

This work was supported in part by the Austrian *Fonds zur Förderung der Wissenschaftlichen Forschung*, Proj. P14094-MAT.

References

[1] A. T. Balaban, D. Fărcaşiu, and R. Bănică. Graphs of multiple 1,2-shifts in carbonium ions and related systems. *Rev. Roum. Chem.*, 11:1205–1227, 1966.

[2] R. Balducci and R. S. Pearlman. Efficient exact solution of the ring perception problem. *J. Chem. Inf. Comput. Sci.*, 34:822–831, 1994.

[3] C. Berge. *Graphs.* North-Holland, Amsterdam, NL, 1985.

[4] B. Bollobás. *Modern Graph Theory.* Springer, New York, 1998.

[5] L. O. Chua and L. Chen. On optimally sparse cycle and coboundary basis for a linear graph. *IEEE Trans. Circuit Theory*, 20:54–76, 1973.

[6] G. M. Downs, V. J. Gillet, J. D. Holliday, and M. F. Lynch. Review of ring perception algorithms for chemical graphs. *J. Chem. Inf. Comput. Sci.*, 29:172–187, 1989.

[7] D. A. Fell. *Understanding the Control of Metabolism.* Portland Press, London, 1997.

[8] A. Galluccio and M. Loebl. (p, q)-odd graphs. *J. Graph Theory*, 23(2):175–184, 1996.

[9] P. M. Gleiss, P. F. Stadler, A. Wagner, and D. A. Fell. Relevant cycles in chemical reaction network. *Adv. Cmplx. Syst.*, 4, 2001. in press.

[10] M. Hartmann, H. Schneider, and M. H. Schneider. Integral bases and p-twisted digraphs. *Europ. J. Combinatorics*, 16:357–369, 1995.

[11] D. Hartvigsen. Minimum path bases. *J. Algorithms*, 15:125–142, 1993.

[12] D. Hartvigsen and R. Mardon. When do short cycles generate the cycle space. *J. Comb. Theory, Ser. B*, 57:88–99, 1993.

[13] D. Hartvigsen and R. Mardon. The all-pair min-cut problem and the minimum cycle basis problem on planar graphs. *SIAM J. Discr. Math.*, 7:403–418, 1994.

[14] J. D. Horton. A polynomial-time algorithm to find the shortest cycle basis of a graph. *SIAM J. Comput.*, 16:359–366, 1987.

[15] D. B. Johnson. Finding all the elementary circuits of a directed graph. *SIAM J. Comput.*, 4:77–84, 1975.

[16] A. Kaveh. *Structural Mechanics: Graph and Matrix Methods.* Research Studies Press, Exeter, UK, 1992.

[17] J. B. Kruskal. On the shortest spanning subgraph of a graph and the travelling salesman problem. *Proc. Amer. Math. Soc.*, 7:48–49, 1956.

[18] M. Las Vergnas. Sur le nombre de circuits dans un tournnoi fortement connexe. *Cahiers C.E.R.O.*, 17:261–265, 1975.

[19] D. Marcu. On finding the elementary paths and circuits of a digraph. *Polytech. Univ. Bucharest Sci. Bull. Ser. D: Mech. Engrg.*, 55:29–33, 1993.

[20] R. T. Rockafellar. *Convex Analysis.* Princeton Univ. Press, Princeton NJ, 1970.

[21] G. F. Stepanec. Basis systems of vector cycles with extremal properties in graphs. *Uspekhi Mat. Nauk. 2*, 19:171–175, 1964. (Russian).

[22] K. Thulasiraman and M. N. S. Swamy. *Graphs: Theory and Algorithms.* J. Wiley & Sons, New York, 1992.

[23] P. Visamara. *Reconnaissance et représentation d'éléments structuraux pour la description d'objets complexes. Application à l'élaboration de stratégies de synthèse en chimie organique.* PhD thesis, Université Montpellier II, France, 1995. 95-MON-2-253.

[24] P. Vismara. Union of all the minimum cycle bases of a graph. *Electr. J. Comb.*, 4:73–87, 1997. Paper No. #R9 (15 pages).