PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 122, Number 1, September 1994

A CANONICAL ORDERING FOR FREE SELF-DISTRIBUTIVE SYSTEMS

PATRICK DEHORNOY

(Communicated by Andreas R. Blass)

ABSTRACT. We construct in free left distributive systems a natural relation that corresponds to the lexicographical ordering on sequences and proves to be a linear ordering. Applications to a word problem and to a characterization of free objects are given.

Let Σ be any set. Any linear ordering $<$ on Σ can be extended in a canonical way to the free semigroup generated by Σ so that left translations are compatible with the extended ordering; since this semigroup is represented by the set of all (nonempty) finite sequences from Σ endowed with concatenation, the *lexicographical* ordering derived from $<$ has the desired property.

This simple scheme does not work in general when the associativity identity $x(yz) = (xy)z$ is replaced by another algebraic identity. The aim of this paper is to discuss the case of (one-sided) distributivity $x(yz) = (xy)(xz)$ and to show that, due to very specific properties, the ordering extension scheme above still works in this case.

The interest for such a study originates in the increasing role played by distributive systems in set theory (iterations of an elementary embedding of a rank into itself—see [11, 2, 6]) as well as in topology (automorphic sets, knot quandles, and crystals—see [1, 7, 8]). In the particular case of structures with one generator, a canonical linear ordering was introduced independently in [4] and [10] and proved to be the main tool for analysing the situation and, in particular, for solving the associated word problem. The present paper shows how a convenient lexicographical extension of this ordering can be constructed in the general case. This construction rests upon the criterion established in [3] for proving equivalence of terms in free distributive systems.

The general meaning of the methods developed here seems to be that for free distributive systems the main complexity lies in the case of one generator and that extending the results to the case of several generators does not require new tools. As an application, we describe a simple algorithm that solves the word problem in the general case and give a criterion for proving that a given distributive system is free.

In the sequel, Σ will be any (nonempty) set, and $\Sigma^{\#}$ will denote the free

Received by the editors July 15, 1992 and, in revised form, November 24, 1992.
1991 *Mathematics Subject Classification.* Primary 17A30.

0002-9939/94 $1.00 + $.25 per page

left distributive system generated by Σ, i.e., the free object generated by Σ in the category of all binary systems (i.e., sets endowed with a binary operation) satisfying the left distributivity identity

$$x(yz) = (xy)(xz).$$

As usual, $\Sigma^{\#}$ can be described as the quotient structure of the absolutely free system $\mathcal{T}_\Sigma$ generated by Σ under the least congruence $=_{LD}$ on $\mathcal{T}_\Sigma$ such that, for every u, v, and w in $\mathcal{T}_\Sigma$, $u(vw) =_{LD} (uv)(uw)$ holds.

The elements of $\mathcal{T}_\Sigma$ are called terms. They will be represented as words constructed from Σ and a binary operator, say $\bullet$, using the *right Polish notation*. So the product of u and v is $uv\bullet$, and the left distributivity identity is expressed by the equality $uvw\bullet\bullet = uv\bullet uw\bullet\bullet$. We use $a, b, c, \ldots$ for the elements of Σ and $\alpha, \beta, \gamma, \ldots$ for arbitrary words constructed from Σ and $\bullet$, and reserve $s, t, u, \ldots$ for terms (which are particular words). We write $\alpha \sqsubset \beta$ if α is a strict prefix of β, i.e., if γ is $\alpha\beta$ for some nonempty word β.

The result we prove here is the following one.

Proposition 1. *Let $<$ be a linear ordering on Σ. Then the lexicographical extension of $<$ to $\mathcal{T}_\Sigma$ via right Polish notation induces on $\Sigma^{\#}$ a linear ordering that is compatible with left translations.*

To prove this result, we polarize the symmetric relation $=_{LD}$ into oriented rewriting rules. To this end we introduce a relation $\rightarrow^1$ on $\mathcal{T}_\Sigma$ so that $s \rightarrow^1 t$ holds when t is obtained from s by replacing some subterm $uvw\bullet\bullet$ of s by the corresponding pattern $uv\bullet uw\bullet\bullet$ and let $\rightarrow$ be the reflexive-transitive closure of $\rightarrow^1$. Clearly $=_{LD}$ is the equivalence relation generated by $\rightarrow$. The following lemma summarizes the specific properties of left distributivity which will be used in the sequel. For σ a mapping of Σ into itself, we write u^σ for the term obtained from u by replacing each letter a by the corresponding $\sigma(a)$.

Lemma 2. (i) (*prefix compatibility*) *Assume that u is a prefix of v, say $v = u\beta$. Then $u \rightarrow \overline{u}$ implies $v \rightarrow \overline{u}\beta$, and $v \rightarrow \overline{v}$ implies that $u \rightarrow \overline{u}$ holds for some prefix $\overline{u}$ of $\overline{v}$.*

(ii) (*right invariance*) *Assume that v is $\alpha a\bullet^n$. Then $v \rightarrow \overline{v}$ implies that $\overline{v}$ is $\overline{\alpha}a\bullet^n$ for some word $\overline{\alpha}$; moreover, $\alpha b\bullet^n \rightarrow \overline{\alpha}b\bullet^n$ holds for every b in Σ.*

(iii) (*prefix completion*) *Assume that α is a (word) prefix of v. Then there exists a unique integer n such that $\alpha\bullet^n$ is a term, and then $v \rightarrow \alpha\bullet^n\beta$ holds for some word β.*

(iv) (*substitution*) *Assume that σ is a mapping of Σ into itself and $u^\sigma \rightarrow \overline{v}$ holds. Then $u \rightarrow v$ holds for some term v such that $\overline{v}$ is v^σ.*

(v) (*confluence*) *Assume $u \rightarrow v$ and $u \rightarrow w$. Then $v \rightarrow \overline{u}$ and $w \rightarrow \overline{u}$ hold for some term $\overline{u}$.*

(vi) (*prefix antireflexivity*) *Assume $v \rightarrow w$. Then $v \rightarrow \overline{w}$ cannot hold for any strict prefix $\overline{w}$ of w.*

The five first properties are established in [3]. The last one was first proved by Laver in [10] using a large cardinal hypothesis in set theory. The logical assumption was dropped subsequently in [5]. A shorter proof appears in [12]. It easily follows from the confluence property that $v =_{LD} w$ holds iff for some

term $\overline{u}$ both $v \to \overline{u}$ and $w \to \overline{u}$ hold; two terms are equivalent iff they can be expanded into a common third one by left distributivity.

Definition. (i) The lexicographical extension of $<$ to $\mathcal{T}_\Sigma$ is denoted by $<_{\mathrm{Lex}}$: $v <_{\mathrm{Lex}} w$ holds if either w is $v\gamma$ for some nonempty word γ or v is $\alpha b\beta$ and w is $\alpha c\gamma$ for some words α, β, and γ and some b and c in Σ satisfying $b < c$.

(ii) The $=_{\mathrm{LD}}$-saturation of $<_{\mathrm{Lex}}$ is denoted $<^\sharp$: $v <^\sharp w$ holds if $\hat{v} <_{\mathrm{Lex}} \hat{w}$ holds for some terms $\hat{v}$ and $\hat{w}$ satisfying $v =_{\mathrm{LD}} \hat{v}$ and $w =_{\mathrm{LD}} \hat{w}$.

(iii) Write $v \ll w$ if there exist an integer n, a word α and b and c in Σ such that $\alpha b\bullet^n$ is a prefix of v, $\alpha c\bullet^n$ is a prefix of w, and $b < c$ holds.

Since $v <_{\mathrm{Lex}} w$ implies $uv\bullet <_{\mathrm{Lex}} uw\bullet$, the ordering $<_{\mathrm{Lex}}$ is compatible with left translations. The congruence $=_{\mathrm{LD}}$ is also compatible with left translations, so the relation $<^\sharp$ must be compatible as well. Observe that since the operator $\bullet$ is not in the domain of the relation $<$, the ordering $<_{\mathrm{Lex}}$ is *not* a linear ordering on $\mathcal{T}_\Sigma$; for instance, the terms $ab\bullet ac\bullet\bullet$ and $abc\bullet\bullet$ are incomparable with respect to $<_{\mathrm{Lex}}$. Both $\sqsubset$ and $\ll$ are refinements of $<_{\mathrm{Lex}}$, but $<_{\mathrm{Lex}}$ is more than the union of $\sqsubset$ and $\ll$, for the discrepancy between two terms need not necessarily appear at the last character of a subterm. For instance, $abc\bullet\bullet <_{\mathrm{Lex}} aca\bullet\bullet$ holds, but neither $abc\bullet\bullet \ll aca\bullet\bullet$ nor $abc\bullet\bullet \sqsubset aca\bullet\bullet$ does.

The following criterion mainly follows from the confluence property of $\to$.

Lemma 3. *For v, w in $\mathcal{T}_\Sigma$, $v <^\sharp w$ holds if and only if there exist two terms $\overline{v}$ and $\overline{w}$ such that $v \to \overline{v}$ and $w \to \overline{w}$ hold and either $\overline{v} \sqsubset \overline{w}$ or $\overline{v} \ll \overline{w}$ holds.*

Proof. The condition is clearly sufficient. Conversely assume $v <^\sharp w$, and fix terms $\hat{v}$, $\hat{w}$ such that $v =_{\mathrm{LD}} \hat{v}$, $w =_{\mathrm{LD}} \hat{w}$, and $\hat{v} <_{\mathrm{Lex}} \hat{w}$ hold.

Case 1. $\hat{v} \sqsubset \hat{w}$. By the confluence property, there exists some term v' such that $v \to v'$ and $\hat{v} \to v'$ hold. Now $\hat{v}$ is a prefix of $\hat{w}$, i.e., $\hat{w}$ is $\hat{v}\gamma$ for some nonempty word γ. By prefix compatibility, $\hat{w} \to v'\gamma$ holds. By confluence again, there exists a term $\overline{w}$ such that $w \to \overline{w}$ and $v'\gamma \to \overline{w}$ hold. By prefix compatibility, we conclude that $v' \to \overline{v}$ holds for some prefix $\overline{v}$ of $\overline{w}$. By transitivity, we get $v \to \overline{v}$, and we are done, since $\overline{v}$ cannot be equal to $\overline{w}$, for in that case we would deduce using prefix compatibility that both $v'\gamma \to \overline{w}$ and $v'\gamma \to \overline{w}\gamma$ hold; hence $\overline{w} =_{\mathrm{LD}} \overline{w}\gamma$, in contradiction with prefix antireflexivity.

Case 2. $\hat{v} = \alpha b\beta$ and $\hat{w} = \alpha c\gamma$ for some words α, β, and γ and some b and c in Σ satisfying $b < c$. By prefix completion, there exist words $\hat{\beta}$ and $\hat{\gamma}$ and an integer n such that $\alpha b\bullet^n$ and $\alpha c\bullet^n$ are terms and $\hat{v} \to \alpha b\bullet^n\hat{\beta}$ and $\hat{w} \to \alpha c\bullet^n\hat{\gamma}$ hold. Since v and $\alpha b\bullet^n\hat{\beta}$ are equivalent, there must exist by the confluence property a term v' such that $v \to v'$ and $\alpha b\bullet^n\hat{\beta} \to v'$ hold. By prefix compatibility, there is a prefix u' of v' such that $\alpha b\bullet^n \to u'$ holds, and, by right invariance, u' must be $\alpha' b\bullet^n$ for some word α', so v' is $\alpha' b\bullet^n\overline{\beta}$ for some word $\overline{\beta}$. By the same argument, there exists a term w'' such that $w \to w''$ and $\alpha c\bullet^n\gamma \to w''$ hold, and w'' is $\alpha'' c\bullet^n\overline{\gamma}$ for some words α'' and $\overline{\gamma}$ satisfying $\alpha c\bullet^n \to \alpha'' c\bullet^n$. Now, by right invariance, $\alpha b\bullet^n \to \alpha'' b\bullet^n$ holds as well, so by confluence (and right invariance) there must exist a word $\overline{\alpha}$ such that both $\alpha' b\bullet^n \to \overline{\alpha} b\bullet^n$ and $\alpha'' c\bullet^n \to \overline{\alpha} c\bullet^n$ hold. By prefix compatibility, $v' = \alpha' b\bullet^n\overline{\beta} \to \overline{\alpha} b\bullet^n\overline{\beta}$ and $w'' = \alpha'' c\bullet^n\overline{\gamma} \to \overline{\alpha} c\bullet^n\overline{\gamma}$ follow, and since $\to$ is

transitive, we deduce that both $v \to \overline{\alpha} b \bullet^n \overline{\beta}$ and $w \to \overline{\alpha} c \bullet^n \overline{\gamma}$ hold. This is the desired result since $\overline{\alpha} b \bullet^n \overline{\beta} \ll \overline{\alpha} c \bullet^n \overline{\gamma}$ clearly holds. □

Lemma 4. *The relation $<^\sharp$ is antireflexive.*

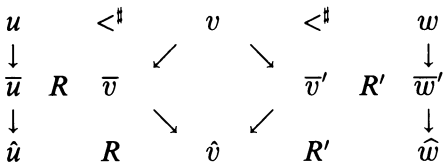
Proof. Assume $u <^\sharp u$. By Lemma 3, there exist two terms $\overline{v}$ and $\overline{w}$ satisfying $u \to \overline{v}$ and $u \to \overline{w}$, and either $\overline{v} \sqsubset \overline{w}$ or $\overline{v} \ll \overline{w}$. The first case directly contradicts the prefix antireflexivity. Assume $\overline{v} \ll \overline{w}$. Write $\overline{v}$ as $\alpha b \bullet^n \beta$ and $\overline{w}$ as $\alpha c \bullet^n \gamma$. By the confluence property, there exists a term v satisfying $\alpha b \bullet^n \beta \to v$ and $\alpha c \bullet^n \gamma \to v$. By prefix compatibility (and right invariance), v can be written as $\alpha' b \bullet^n \beta'$ and $\alpha'' c \bullet^n \gamma''$ for some words α', β', α'', and γ'' satisfying $\alpha b \bullet^n \to \alpha' b \bullet^n$ and $\alpha c \bullet^n \to \alpha'' c \bullet^n$. Since b and c are different members of Σ, α' and α'' cannot be the same prefix of v. So assume, for instance, that α' is a strict prefix of α''. Then $\alpha' b \bullet^n$ is a strict prefix of $\alpha'' b \bullet^n$. But $\alpha b \bullet^n \to \alpha' b \bullet^n$ was assumed, and $\alpha b \bullet^n \to \alpha'' b \bullet^n$ follows from $\alpha c \bullet^n \to \alpha'' c \bullet^n$ by right invariance, contradicting the prefix antireflexivity. In both cases we have a contradiction. □

Lemma 5. *Let R be $\sqsubset$, $\sqsupset$, $\ll$, or $\gg$, and assume $s R t$ and $t \to \hat{t}$. Then for some term $\hat{s}$ both $s \to \hat{s}$ and $\hat{s} R \hat{t}$ hold.*

Proof. If R is $\sqsubset$ or $\sqsupset$, the result is just prefix compatibility as stated above. Assume that R is $\ll$ or $\gg$. Then s is $\alpha b \bullet^n \beta$ and t is $\alpha c \bullet^n \gamma$ for some integer n, some words α, β, and γ, and some b and c in Σ such that $\alpha b \bullet^n$ is a term and $b < c$ (resp. $c < b$) holds if R is $\ll$ (resp. $\gg$). By prefix compatibility, there is a prefix $\hat{u}$ of $\hat{t}$ satisfying $\alpha c \bullet^n \to \hat{u}$, and by right invariance $\hat{u}$ is $\hat{\alpha} c \bullet^n$ for some word $\hat{\alpha}$. Then $\alpha b \bullet^n \to \hat{\alpha} b \bullet^n$ holds, and $s \to \hat{\alpha} b \bullet^n \beta$ follows. Now $\hat{\alpha} b \bullet^n \beta \ll \hat{t}$ (resp. $\hat{t} \ll \hat{\alpha} b \bullet^n \beta$) holds if $b < c$ (resp. $c < b$) does. □

Lemma 6. *The relation $<^\sharp$ is transitive.*

Proof. Assume $u <^\sharp v <^\sharp w$. By Lemma 3, there exist terms $\overline{u}$, $\overline{v}$, $\overline{v}'$ and $\overline{w}'$ such that one has simultaneously $u \to \overline{u}$, $v \to \overline{v}$, $v \to \overline{v}'$, $w \to \overline{w}'$, $\overline{u} R \overline{v}$, and $\overline{v}' R' \overline{w}'$ where R and R' are either $\sqsubset$ or $\ll$. The first step is to reduce to the case where $\overline{v}$ and $\overline{v}'$ are equal. By the confluence property, there exists a term $\hat{v}$ such that both $\overline{v} \to \hat{v}$ and $\overline{v}' \to \hat{v}$ hold. Applying Lemma 5 to $\overline{u}$, $\overline{v}$, $\hat{v}$, and R, we get a term $\hat{u}$ satisfying $\overline{u} \to \hat{u}$ (and therefore $u \to \hat{u}$) and $\hat{u} R \hat{v}$. Then applying Lemma 5 to $\overline{v}'$, $\overline{w}'$, $\hat{v}$, and R'^{-1}, we get a term $\hat{w}$ satisfying $\overline{w}' \to \hat{w}$ (and therefore $w \to \hat{w}$) and $\hat{v} R' \hat{w}$.



It remains to consider the four possible cases.

Case 1. $\hat{u} \sqsubset \hat{v} \sqsubset \hat{w}$. Then $\hat{u} \sqsubset \hat{w}$ obviously follows.

Case 2. $\hat{u} \sqsubset \hat{v} \ll \hat{w}$. Then $\hat{v}$ is $\alpha b \bullet^n \beta$ and $\hat{w}$ is $\alpha c \bullet^n \gamma$ for some α, β, γ, b, c, and n with $b < c$. Then either $\hat{u}$ is a strict prefix of $\alpha b \bullet^n$, hence of α and $\hat{w}$ as well, or $\alpha b \bullet^n$ is a prefix of $\hat{u}$, and $\hat{u} \ll \alpha c \bullet^n \hat{\gamma}$ follows.

Case 3. $\hat{u} \ll \hat{v} \sqsubset \hat{w}$. Then $\hat{u} \ll \hat{w}$ is obviously true.

Case 4. $\hat{u} \ll \hat{v} \ll \hat{w}$. Then $\hat{u}$ is $\alpha b \bullet^n \beta$, $\hat{v}$ is $\alpha c \bullet^n \gamma$, and $\alpha' b' \bullet^{n'} \beta'$ and $\hat{w}$ is $\alpha' c' \bullet^{n'} \gamma'$ for some α, β, γ, b, c, n, α', β', γ', b', c', and n' with $b < c$

and $b' < c'$. If α is a strict prefix of α', $\alpha c \bullet^n$ is a prefix of $\hat{w}$, and $\hat{u} \ll \hat{w}$ follows from $b < c$. If α and α' are equal, c and b' coincide, and therefore $b < c'$ holds, so $\hat{u} \ll \hat{w}$ follows. Finally, if α' is a strict prefix of α, $\alpha' b' \bullet^{n'}$ is a prefix of $\hat{u}$, and $\hat{u} \ll \hat{w}$ follows from $b' < c'$.

So, in each case, $\hat{u} <^\sharp \hat{w}$ holds and $u <^\sharp w$ follows. □

It follows that the relation $<^\sharp$ is a strict ordering on $\mathscr{T}_\Sigma$. Since this relation has been made compatible with the equivalence relation $=_{LD}$, it induces a well-defined strict ordering on the quotient set $\Sigma^\sharp$. It remains to prove that this ordering is linear. We shall make use of the results proved in [4] for the case of one generator.

Lemma 7. *The relation $<^\sharp$ induces a linear ordering on $\Sigma^\sharp$.*

Proof. Let a be a fixed element of Σ, and let π be the projection of $\mathscr{T}_\Sigma$ onto $\mathscr{T}_{\{a\}}$ which maps every element of Σ to a. Let v and w be arbitrary terms in $\mathscr{T}_\Sigma$. It is proved in [4] that there exist two terms $\overline{v}$ and $\overline{w}$ in $\mathscr{T}_{\{a\}}$ such that $v^\pi \to \overline{v}$ and $w^\pi \to \overline{w}$ hold and either $\overline{v}$ and $\overline{w}$ are equal or one is a prefix of the other. By substitution, there exist two terms $\hat{v}$ and $\hat{w}$ in $\mathscr{T}_\Sigma$ such that $v \to \hat{v}$ and $w \to \hat{w}$ hold and $\overline{v}$ (resp. $\overline{w}$) is $\hat{v}^\pi$ (resp. $\hat{w}^\pi$). It follows that $\hat{v}$ and $\hat{w}$ must be comparable for $<_{Lex}$. Indeed two terms are $<_{Lex}$-incomparable just in case their leftmost discrepancy as words has type "an element of Σ versus $\bullet$" or conversely, and such a discrepancy would then still occur on the projected terms $\overline{v}$ and $\overline{w}$, contradicting the hypothesis that one of them is a prefix of the other. Therefore, v and w are $<^\sharp$-comparable. □

Proposition 1 is thus proved. As an application, we can extend to the general case the algorithm given in [4] in the case of one single generator for solving the word problem for $=_{LD}$ on $\mathscr{T}_\Sigma$. Assume that v and w are arbitrary terms in $\mathscr{T}_\Sigma$. In order to decide whether $v =_{LD} w$ holds, enumerate all pairs $(\overline{v}, \overline{w})$ satisfying $v \to \overline{v}$ and $w \to \overline{w}$. By Lemma 3, a pair $(\overline{v}, \overline{w})$ will eventually appear such that either $\overline{v}$ and $\overline{w}$ are equal or $\overline{v} <_{Lex} \overline{w}$ or $\overline{w} <_{Lex} \overline{v}$ holds. In the first case one can conclude that $v =_{LD} w$ is true; in both remaining cases one can conclude that $v =_{LD} w$ is false.

Another application is the following criterion, which extends to the general case the criterion used by Laver in [10] for proving the freeness of a left distributive system in the case of a single generator.

Proposition 8. *Assume that $\mathfrak{g}$ is a left distributive system generated by a set Σ. Then $\mathfrak{g}$ is the free left distributive system generated by Σ iff any equality of one of the following types is impossible in $\mathfrak{g}$:*

$$x = xy_1 \bullet y_2 \bullet \cdots y_q \bullet \text{ with } q \text{ a positive integer,}$$

$$x_1 x_2 \cdots x_p b \bullet^p y_1 \bullet \cdots y_q \bullet = x_1 x_2 \cdots x_p c \bullet^p z_1 \bullet \cdots z_r \bullet, \text{ with } p, q, \text{ and } r \text{ nonnegative integers and } b \text{ and } c \text{ distinct elements of } \Sigma.$$

Proof. Let π be the surjective homomorphism of $\Sigma^\sharp$ onto $\mathfrak{g}$ which is the identity on Σ. For proving that π is injective it suffices to show that $v <^\sharp w$ implies $v^\pi \neq w^\pi$. From the definition of $<^\sharp$ it suffices to show the implication when $v \sqsubset w$ or $v \ll w$ holds, and this is exactly what the conditions in the statement express. □

References

1. E. Brieskorn, *Automorphic sets and braids and singularities*, Braids, Contemp. Math., vol. 78, Amer. Math. Soc., Providence, RI, 1988, pp. 45–117.
2. P. Dehornoy, Π^1_1*-complete families of elementary sequences*, Ann. Pure Appl. Logic **38** (1988), 1–31.
3. ——, *Free distributive groupoids*, J. Pure Appl. Algebra **61** (1989), 123–146.
4. ——, *Sur la structure des gerbes libres*, C. R. Acad. Sci. Paris Sér. I Math. **309** (1989), 143–148.
5. ——, *Preuve de la conjecture d' irréflexivité pour les structures distributives libres*, C. R. Acad. Sci. Paris Sér. I. Math. **314** (1992), 333–336.
6. R. Dougherty, *Critical points of elementary embeddings*, preprint, 1989.
7. D. Joyce, *A classifying invariant of knots: the knot quandle*, J. Pure Appl. Algebra **23** (1982), 37–65.
8. L. Kauffmann, *Knots and physics*, World Scientific, Singapore, 1991.
9. P. Kepka, *Notes on left distributive groupoids*, Acta Univ. Carolin.—Math. Phys. **22** (1981), 23–37.
10. R. Laver, *The left distributive law and the freeness of an algebra of elementary embeddings*, Adv. Math. **91** (1992), 209–231.
11. ——, *On the algebra of elementary embeddings of a rank into itself*, Adv. Math. (to appear).
12. D. Larue, *On braid words and irreflexivity*, Univ. Algebra (to appear).

Departement de Mathématiques, Université de Caen, 14032 Caen cedex, France
E-mail address: dehornoy@geocub.greco-prog.fr