Αξιωματικές αποδείξεις καθολικών κάτω φραγμάτων

Γιάννης Ν. Μοσχοβάκης
UCLA και ΕΚΠΑ

Ηράκλειο, 20 Μαΐου 2008

'Ενα κάτω φράγμα

Θεώρημα (van den Dries, ΓΝΜ)

Αν ο αλγόριθμος α αποφασίζει τη σχέση της «σχετικής πρωτότητας» (coprimeness) $x \perp\!\!\!\perp y$ στο $\mathbb{N} = \{0, 1, \ldots\}$ από τα δοσμένα $\leq, +, \dot{-}, \mathrm{iq}, \mathrm{rem}$, τότε για άπειρα το πλήθος ζεύγη a, b

$$c^s_\alpha(a, b) > \frac{1}{10} \log\log(\max(a, b)) \qquad (*)$$

[Η (*) ισχύει για όλες τις λύσεις της εξίσωσης του Pell, $a^2 = 1 + 2b^2$]

- $\mathrm{iq}(x, y), \mathrm{rem}(x, y)$ είναι το πηλίκο και το υπόλοιπο
- Η $c^s_\alpha(x, y)$ μετρά τις εφαρμογές των δοσμένων στον υπολογισμό
- Ισχυρισμός: Το αποτέλεσμα ισχύει για όλους τους αλγόριθμους από τα δοσμένα
- Ο Ευκλείδειος αλγόριθμος ε αποφασίζει τη σχέση $x \perp\!\!\!\perp y$ (από την rem μόνο) με πολυπλοκότητα

$$c^s_\varepsilon(a, b) \leq 2\log(\min(a, b)) \quad (\min(a, b) \geq 2)$$

Περίληψη

Slogan: *Τα καθολικά κάτω φράγματα είναι*
τα γεγονότα αναποκρισιμότητας για επιλύσιμα προβλήματα
...και θα έπρεπε η λογική να έχει κάτι να πει γι' αυτά!

(1) Μικρή επέμβαση στη λογική, έτσι που να εφαρμόζεται εύκολα στη θεωρία υπολογισμού
(2) Τρία (απλά) αξιώματα για αλγόριθμους (στο στυλ της *αφηρημένης μοντελοθεωρίας*)
(3) Κάτω φράγματα από τα αξιώματα

Is the Euclidean algorithm optimal among its peers? (with vDD, 2004)
Arithmetic complexity (with vDD, to appear)

Μερικές άλγεβρες, εμφυτεύσεις και υποάλγεβρες

- (Μερική) **άλγεβρα** είναι η τυχαία δομή $\mathbf{M} = (M, 0, 1, \Phi^{\mathbf{M}})$ όπου $0, 1 \in M$, το Φ είναι σύνολο συναρτησιακών συμβόλων και $\Phi^{\mathbf{M}} = \{\phi^{\mathbf{M}}\}_{\phi \in \Phi}$, με $\phi^{\mathbf{M}} : M^{n_\phi} \rightharpoonup M$ για κάθε $\phi \in \Phi$

- **Εμφύτευση** $\iota : \mathbf{U} \rightarrowtail \mathbf{M}$ από μια Φ-άλγεβρα σε μιαν άλλη είναι η τυχαία 1-1 συνάρτηση $\iota : U \rightarrowtail M$ τέτοια που

$$\iota(0^{\mathbf{U}}) = 0^{\mathbf{M}}, \quad \iota(1^{\mathbf{U}}) = 1^{\mathbf{M}},$$

και για κάθε $\phi \in \Phi, x_1, \ldots, x_n, w \in U$,

$$\phi^{\mathbf{U}}(x_1, \ldots, x_n) = w \implies \phi^{\mathbf{M}}(\iota x_1, \ldots, \iota x_n) = \iota w$$

- $\mathbf{U} \subseteq_p \mathbf{M}$ αν η ταυτοτική $I : U \rightarrowtail M$ είναι εμφύτευση

Περιορισμοί

$\mathbf{N}_\varepsilon = (\mathbb{N}, 0, 1, \mathrm{rem})$, η άλγεβρα του Ευκλείδειου
$\mathbf{N}_u = (\mathbb{N}, 0, 1, S, \mathrm{Pd})$ (*unary numbers*)
$\mathbf{N}_b = (\mathbb{N}, 0, 1, \mathrm{Parity}, \mathrm{iq}_2, (x \mapsto 2x), (x \mapsto 2x+1))$, (*binary numbers*)

Για $\mathbf{M} = (M, 0, 1, \Phi^{\mathbf{M}})$ και $\{0,1\} \subseteq U \subseteq M$, θέτουμε

$$\mathbf{M} \restriction U = (U, 0, 1, \Phi^{\mathbf{U}}),$$

όπου για $\phi \in \Phi$,

$$\phi^{\mathbf{U}}(\vec{x}) = w \iff \vec{x}, w \in U \;\&\; \phi^{\mathbf{M}}(\vec{x}) = w$$

Για πεπερασμένο $U \subset \mathbb{N}$, η $\mathbf{N}_u \restriction U$ είναι πεπερασμένη, γνήσια-μερική υποάλγεβρα της $\mathbf{N}_u$

Υποάλγεβρες που παράγονται από την είσοδο

$$\mathbf{M} = (M, 0, 1, \Phi^{\mathbf{M}})$$

Για $\vec{x} = x_1, \ldots, x_n \in M$, θέτουμε

$$G_0(\vec{x}) = \{0, 1, x_1, \ldots, x_n\}$$
$$G_{m+1}(\vec{x}) = G_m(\vec{x}) \cup \{\phi^{\mathbf{M}}(\vec{u}) \mid \phi \in \Phi, \vec{u} \in G_m(\vec{x}) \text{ και } \phi^{\mathbf{M}}(\vec{u})\downarrow\}$$

έτσι που

$$G_m(\vec{x}) = \{t^{\mathbf{M}}[x_1, \ldots, x_n] \in M \mid \text{ ο } t(v_1, \ldots, v_n) \text{ είναι όρος βάθους } \leq m\}$$

$\boxed{\mathbf{M} \restriction G_m(\vec{x}) \text{ είναι η υποάλγεβρα βάθους } m \text{ που παράγεται από την } \vec{x}}$

$(\mathbf{M} \restriction \bigcup_m G_m(\vec{x})$ είναι η υποάλγεβρα που παράγεται από την $\vec{x})$

I Αξίωμα Τοπικότητας ή Σχετικοποίησης (Locality)

Κάθε αλγόριθμος α πλειομέλειας n της άλγεβρας $\mathbf{M} = (M, 0, 1, \Phi^{\mathbf{M}})$ *καθορίζει σε κάθε υποάλγεβρα* $\mathbf{U} \subseteq_p \mathbf{M}$ *μία n-μελή μερική συνάρτηση*

$$\overline{\alpha}^{\mathbf{U}} : U^n \rightharpoonup U$$

- Οι **M**-αλγόριθμοι «υπολογίζουν μερικές συναρτήσεις», και ερμηνεύονται σε τυχαίες υποάλγεβρες της **M**

Χρησιμοποιούμε το συμβολισμό

$$\boxed{\mathbf{U} \models \overline{\alpha}(\vec{x}) = w \iff \vec{x} \in U^n, w \in U \text{ and } \overline{\alpha}^{\mathbf{U}}(\vec{x}) = w}$$

II Αξίωμα Εμφύτευσης (Embedding)

Αν ο α είναι n-μελής αλγόριθμος της $\mathbf{M}$, $\quad \mathbf{U}, \mathbf{V} \subseteq_p \mathbf{M}$, *και* $\iota : \mathbf{U} \rightarrowtail \mathbf{V}$ *είναι εμφύτευση, τότε*

$$\mathbf{U} \models \overline{\alpha}(\vec{x}) = w \implies \mathbf{V} \models \overline{\alpha}(\iota\vec{x}) = \iota w \quad (x_1, \ldots, x_n, w \in U)$$

Ειδικότερα, αν $\mathbf{U} \subseteq_p \mathbf{M}$, τότε $\overline{\alpha}^{\mathbf{U}} \subseteq \overline{\alpha}^{\mathbf{M}}$

- Οι αλγόριθμοι χρησιμοποιούν τα δοσμένα της $\mathbf{M}$ ως *μαντεία*: ζητούν τιμές $\phi^{\mathbf{M}}(\vec{y})$ και τις χρησιμοποιούν (αν τους δοθούν)

III Αξίωμα Περατότητας (Finiteness)

Για κάθε n-μελή αλγόριθμο α *της* **M** *και όλα τα* $\vec{x}, w$,

$$\mathbf{M} \models \overline{\alpha}(\vec{x}) = w \implies \text{υπάρχει κάποιος } m \text{ τέτοιος που } \vec{x}, w \in G_m(\vec{x})$$
$$\text{και } \mathbf{M} \restriction G_m(\vec{x}) \models \overline{\alpha}(\vec{x}) = w$$

Ειδικότερα,

$$\overline{\alpha}^{\mathbf{M}}(\vec{x})\downarrow \implies \overline{\alpha}(\vec{x}) \in \bigcup_m G_m(\vec{x})$$

- «Ο υπολογισμός» της τιμής $\overline{\alpha}^{\mathbf{M}}(\vec{x})$ γίνεται μέσα στην υποάλγεβρα της **M** που παράγεται από την είσοδο, και είναι πεπερασμένος: το m είναι αρκετά μεγάλο έτσι που κάθε y που «χρησιμοποιείται στον υπολογισμό» ανήκει στην $G_m(\vec{x})$

Όλοι οι γνωστοί αλγόριθμοι ικανοποιούν τα αξιώματα I – III

- Ρητός υπολογισμός: $\overline{\alpha}^{\mathbf{U}}(\vec{x}) = t^{\mathbf{U}}[\vec{x}]$, όπου ο $t(\vec{v})$ είναι Φ-όρος
- $\overline{\alpha}^{\mathbf{U}}$ είναι η μερική συνάρτηση που υπολογίζεται από ένα αναδρομικό πρόγραμμα στο λεξιλόγιο Φ
- Η $\overline{\alpha}^{\mathbf{U}}$ υπολογίζεται από μια μηχανή RAM από τα δοσμένα $\Phi^{\mathbf{U}}$
- Η $\overline{\alpha}^{\mathbf{U}}$ υπολογίζεται στη γλώσσα προγραμματισμού PCF του Plotkin, «επάνω» από την άλγεβρα **U**
- Η $\overline{\alpha}^{\mathbf{U}}$ υπολογίζεται από αναιτιοκρατικές εκδοχές των παραπάνω

• Μηχανές Turing (και παραπλήσια πολύ απλοϊκά μοντέλα υπολογισμού) *προσομοιώνονται πιστά* από αλγόριθμους που ικανοποιούν τα I – III, έτσι που τα καθολικά κάτω φράγματα που συνάγονται από τα αξιώματα ισχύουν και γι' αυτές.

Αξιώματα για απλούς (πρωτοβάθμιους) αλγόριθμους

- I Αξίωμα Τοπικότητας:

  Κάθε αλγόριθμος α *πλειομέλειας* n *της άλγεβρας* $\mathbf{M} = (M, 0, 1, \Phi^{\mathbf{M}})$ *καθορίζει σε κάθε υποάλγεβρα* $\mathbf{U} \subseteq_p \mathbf{M}$ *μία* n*-μελή μερική συνάρτηση*

  $$\overline{\alpha}^{\mathbf{U}} : U^n \rightharpoonup U$$

- II Αξίωμα Εμφύτευσης:

  Αν ο α *είναι* n*-μελής αλγόριθμος της* $\mathbf{M}$*,* $\quad \mathbf{U}, \mathbf{V} \subseteq_p \mathbf{M}$*, και* $\iota : \mathbf{U} \rightarrowtail \mathbf{V}$ *είναι εμφύτευση, τότε*

  $$\mathbf{U} \models \overline{\alpha}(\vec{x}) = w \implies \mathbf{V} \models \overline{\alpha}(\iota\vec{x}) = \iota w \quad (x_1, \ldots, x_n, w \in U)$$

- III Αξίωμα Περατότητας:

  Για κάθε n*-μελή αλγόριθμο* α *της* $\mathbf{M}$*,*

$$\mathbf{M} \models \overline{\alpha}(\vec{x}) = w \implies \text{υπάρχει κάποιος } m \text{ τέτοιος που } \vec{x}, w \in G_m(\vec{x}) \\ \text{και } \mathbf{M} \restriction G_m(\vec{x}) \models \overline{\alpha}(\vec{x}) = w$$

Η πολυπλοκότητα εμφύτευσης ενός αλγόριθμου

Για τυχαίο αλγόριθμο α της $\mathbf{M}$, αν $\mathbf{M} \models \overline{\alpha}(\vec{x}) = w$, θέτουμε

$$\boxed{c^{\iota}_{\alpha}(\vec{x}) = \text{ο ελάχιστος } m \text{ τέτοιος που } \mathbf{M} \restriction G_m(\vec{x}) \models \overline{\alpha}(\vec{x}) = w}$$

Ο ορισμός δικαιολογείται από το Αξίωμα Περατότητας

- Διαισθητικά, αν $m = c^{\iota}_{\alpha}(\vec{x})$, τότε κάθε υλοποίηση του α θα χρειαστεί «να δει» (χρησιμοποιήσει) κάποιο $u \in M$ βάθους m; και επομένως θα χρειαστεί τουλάχιστον m βήματα για να κατασκευάσει αυτό το u από την είσοδο με τα δοσμένα
- Αν $\overline{\alpha}(\vec{x}) = t^{\mathbf{M}}[\vec{x}]$, τότε $c^{\iota}_{\alpha}(\vec{x}) \leq \text{depth}(t(\vec{v}))$
- Η πολυπλοκότητα c^{ι}_{α} είναι μικρότερη από όλες τις συνηθισμένες συναρτήσεις πολυπλοκότητας χρόνου στα γνωστά υπολογιστικά μοντέλα

Η πολυπλοκότητα εμφύτευσης (υπολογίσιμης) συνάρτησης

Η εμφύτευση $\iota : \mathbf{M} \restriction G_m(\vec{x}) \rightarrowtail \mathbf{M}$ σέβεται την $f : M^n \to M$ στο $\vec{x}$ αν

$$f(\vec{x}) \in G_m(\vec{x}) \;\&\; \iota(f(\vec{x})) = f(\iota(\vec{x}))$$

Λήμμα

Αν κάποιος αλγόριθμος υπολογίζει την f στην $\mathbf{M}$, τότε για κάθε $\vec{x}$, υπάρχει κάποιος m τέτοιος που κάθε εμφύτευση $\iota : \mathbf{M} \restriction G_m(\vec{x}) \rightarrowtail \mathbf{M}$ σέβεται την f στο $\vec{x}$

Απόδειξη Έστω $m = c^{\iota}_{\alpha}(\vec{x})$ για κάποιον α που υπολογίζει την f

$$\boxed{c^{\iota}_{f}(\vec{x}) = \text{ο ελάχιστος } m, \text{ τ.π. κάθε } \iota : \mathbf{M} \restriction G_m(\vec{x}) \rightarrowtail \mathbf{M} \text{ σέβεται την } f \text{ στο } \vec{x}}$$

Αν ο α υπολογίζει την f στην $\mathbf{M}$, τότε $c^{\iota}_{f}(\vec{x}) \leq c^{\iota}_{\alpha}(\vec{x})$

- Για να δείξουμε ότι ο m είναι καθολικό κάτω φράγμα για τον υπολογισμό της $f(\vec{x})$, είτε δείχνουμε ότι $\boxed{f(\vec{x}) \notin G_m(\vec{x})}$, είτε κατασκευάζουμε $\iota : \mathbf{M} \restriction G_m(\vec{x}) \rightarrowtail \mathbf{M}$ τ.π., $\boxed{\iota f(\vec{x}) \neq f(\iota \vec{x})}$

Outline of a proof

Θεώρημα (van den Dries, ynm)

For the algebra $\mathbf{M} = (\mathbb{N}, 0, 1, \leq, +, \dot{-}, \mathrm{iq}, \mathrm{rem})$ *and the relation of coprimeness* $x \perp\!\!\!\perp y$,

$$a^2 = 1 + 2b^2 \implies c^{\iota}_{\perp\!\!\!\perp}(a, b) > \frac{1}{10} \log \log(a) \qquad (*)$$

So if α *decides coprimeness in* $\mathbf{M}$, *then* (*) *holds with* $c^{\iota}_{\alpha}(a, b)$

- If $2^{2^{4m+6}} \leq a$, then every $X \in G_m(a, b)$ can be written uniquely as

$$X = \frac{x_0 + x_1 a + x_2 b}{x_3} \qquad \text{with } x_i \in \mathbb{Z}, \quad |x_i| \leq 2^{2^{4m}}$$

and we can define $\iota : \mathbf{M} \restriction G_m(a, b) \rightarrowtail \mathbf{M}$ using $\lambda = 1 + a!$,

$$\iota(X) = \frac{x_0 + x_1 \lambda a + x_2 \lambda b}{x_3}, \text{ so } (\iota(a), \iota(b)) = (\lambda a, \lambda b)$$

$\mathbf{M} = (\mathbb{N}, 0, 1, \mathrm{Parity}, \mathrm{iq}_2, \leq, +, \dot{-}, \text{Presburger functions})$

- (van den Dries, ynm) *If $R(x)$ is one of the relations*

  $$x \text{ is prime}, \quad x \text{ is a perfect square}, \quad x \text{ is square free},$$

  then for some $r > 0$ and infinitely many a, $c^{\iota}_{R}(a) > r\log(a)$

- (van den Dries, ynm) *For some $r > 0$ and infinitely many a, b,*

  $$c^{\iota}_{\perp\!\!\!\perp}(a, b) > r\log(\max(a, b))$$

- (Joe Busch) *If $R(x, p) \iff x$ is a square $\bmod p$,*
  then for some $r > 0$ and a sequence (a_n, p_n) with $p_n \to \infty$,

  $$c^{\iota}_{R}(a_n, p_n) > r\log(p_n)$$

In the last two examples, the results match up to a multiplicative constant the known binary algorithms, so these are optimal

Primality in $\mathbf{M} = (\mathbb{N}, 0, 1, \text{Parity}, \text{iq}_2, \leq, +, \dot{-}, \text{Presburger})$

Θεώρημα (van den Dries, ynm)

If $\text{Prime}(p) \iff p$ is prime, *then in* $\mathbf{M}$, *for some* $r > 0$ *and all primes* p,

$$c^{\iota}_{\text{Prime}}(p) > r \log p \qquad (*)$$

So if α *decides primality in* $\mathbf{M}$, *then* (*) *holds with* $c^{\iota}_{\alpha}(p)$

- If $2^{2m+2} \leq a$, then every $X \in G_m(a)$ can be written uniquely as

$$X = \frac{x_0 + x_1 a}{2^m} \quad \text{with } |x_i| \leq 2^{2m},$$

and we can define $\iota : \mathbf{M} \restriction G_m(a) \rightarrowtail \mathbf{M}$ by

$$\iota(X) = \frac{x_0 + x_1 \lambda a}{2^m}, \text{ with } \lambda = 1 + 2^m, \text{ so } \iota(a) = \lambda a$$

Primality in binary

- If $\mathrm{Prime}(p) \iff p$ is prime, then in

$$\mathbf{N}_b = (\mathbb{N}, 0, 1, \mathrm{Parity}, \mathrm{iq}_2, (x \mapsto 2x), (x \mapsto 2x+1))$$

for some $r > 0$ and all primes p,

$$c^{\iota}_{\mathrm{Prime}}(p) \geq r \log p \tag{*}$$

- This should follow trivially from number-theoretic results, because it takes at least i applications of the primitives of $\mathbf{N}_b$ to read i bits of the input; we should have $r = 1$
- Theorem (Tao). *For infinitely many primes p, if p' is constructed by changing any bit in the binary expansion of p except the highest, then p' is not prime*
- Tao found subsequently that this result is implicit in a paper of Cohen and Selfridge from 1975 and explicitly noted in a 2000 paper by Sun, and he obtained more general results