Aplikace matematiky

Tamás Frey

Über die Optimierung von numerischen Algorithmen

Aplikace matematiky, Vol. 13 (1968), No. 1, 39--43

Persistent URL: http://dml.cz/dmlcz/103137

ÜBER DIE OPTIMIERUNG VON NUMERISCHEN ALGORITHMEN

TAMAS FREY

Die Literatur über Optimierungsfragen von Rechenprozessen ist so umfangreich, dass man sie sehr schwer zusammenfassen kann. Jedoch fast alle Arbeiten beschränken sich in Zusammenhang mit angegebenen Aufgabentypen auf eine annähernde Lösungsmethode, und die Optimierung bedeutet dann eine gute Wahl von gewissen Parametern des betrachteten Algorithmentyps. Erst BABUŠKA und SOBOLEV haben – undzwar eben hier, drei Jahre vorher – die Frage so gestellt: wie gross ist der Operationsbedarf des besten numerischen Algorithmus bei genug scharf charakterisierten Aufgabentypen mit angegebenen Pünktlichkeitsforderungen [1]. Man kann natürlich gleich fragen: wie kann man diesen besten Algorithmus charakterisieren? Babuška und Sobolev haben für die erste Frage untere Grenzen mit Hilfe informationstheoretischer Überlegungen angegeben. Wir kehren zu diesen Überlegungen zurück, um die theoretischen Fragezeichen näher zu zeigen. Betrachten wir jedoch erst die zweite Frage, womit man theoretisch sicher weiter gelangt. Den Weg hat RUTLEDGE geöffnet [2]; er hat nämlich die Arbeit von JANOV über Operator- bzw. Algorithmenschemen in der Sprache der Automatentheorie abgefasst, und die Äquivalenz solcher Schemen mit automatentheoretischen Hilfsmitteln gelöst. Die von Rutledge ausgearbeitete Methode ist jedoch für unsere Zwecke nicht anwendbar, da er die Äquivalenz zweier Schemen im Janovschen Sinne zeigen wollte, d.h. im Sinne, dass zwei äquivalenten Algorithmenschemen für alle möglichen Applikationen dieselbe Abbildung realisieren sollen. Uns interessiert aber eine solche Äquivalenz zweiter Algorithmenschemen, wo die betrachteten Schemen nur in Hinsicht einer angegebenen Applikation dieselbe Abbildung realisieren, um die beste – d.h. schnellste – zwischen den in dieser Hinsicht äquivalenten, auszuwählen.

Die betrachtete Anwendung (Applikation) soll in dieser Konzeption durch einen sog. Mealyschen Pseudoanfangsautomaten (s. [3]), d.h. durch eine Sechstupel $W(\mathfrak{B}, X, Y, \varphi, \psi, \mathfrak{B}_0)$ angegeben werden, wo $X = \{x_1, x_2, \ldots, x_m\}$ die Menge der Inputcharakters bezeichnet (welche im semantischen Sinne den möglichen Operationsbefehlen entsprechen), $Y = \{y_1, \ldots, y_n\}$ ist die Menge der Outputcharakters (im semantischen Sinne die Ergebnisse der logischen Entscheidungen), $\mathfrak{B}$ bezeichnet die Menge der inneren Zustände von W (im semantischen Sinne entspricht einem jeden Zustand $v \in \mathfrak{B}$ eine Datenmenge), $\mathfrak{B}_0 \subseteq \mathfrak{B}$ ist die Menge der möglichen

Anfangszustände (im semantischen Sinne entspricht also einem jeden Zustand $v_\alpha^{(0)} \in \mathfrak{V}_0$ eine konkrete Aufgabe der betrachteten Aufgabenklasse; $\mathfrak{V}_0$ selbst repräsentiert also die zu lösende Aufgabenklasse), φ bzw. ψ sind die Durchgangs- bzw. Ausgangsfunktion von W, welche also $\mathfrak{V} \times X$ in $\mathfrak{V}$ bzw. in Y abbilden, und somit die Arbeit des Automaten W abschreiben.

Der betrachtete Algorithmus ist aber hier ein Pseudomealyscher Anfangsautomat A $(\mathfrak{A}, Y, X, f, g, a_0, \tau)$, wo $Y = \{y_1, \ldots, y_n\}$ die Menge der Input – (!), $X = \{x_1, x_2, \ldots, x_m\}$ aber diejenige der Outputcharakters bezeichnet, $\mathfrak{A}$ die Menge der inneren Zuständen, $\tau \subset \mathfrak{A}$ aber die Menge der terminalen (Stop-) Zuständen, $a_0 \in \mathfrak{A}$ den Anfangszustand (diesen Automaten nennen wir „Pseudomealyschen", da er einerseits im Anfangszustand einen „Startzeichen" $\sigma \notin Y$ bekommt, anderseits in den terminalen Zuständen nicht weiter arbeitet). f bzw. g ist die Durchgangs- bzw. Ausgangsfunktion, bildet also $[\mathfrak{A} - (a_0 \cup \tau)] \times Y$ in $\mathfrak{A} - a_0$ bzw. in X ab (daneben ist auch $f(a_0, \sigma)$ und $g(a_0, \sigma)$ angegeben).

Man schaltet nun A und W zusammen; das so zustandekommende Kompaktum $K = A \rightleftarrows W$ arbeitet folgendermassen: im 0-ten Takt A in $f(a_0, \sigma)$ übergeht, und Outputzeichen $g(a_0, \sigma) = x^{(0)}$ abgibt. Im ersten Takt W in $v^{(1)} = \varphi(v^{(0)}, x^{(0)})$ übergeht, und Outputzeichen $y^{(1)} = \psi(v^{(0)}, x^{(0)})$ abgibt; A aber in $a^{(1)} = f(f(a_0, \sigma), y^{(1)})$ übergeht, und Outputzeichen $x^{(1)} = g(f(a_0, \sigma), y^{(1)})$ abgibt. Allgemein im $(s+1)$-ten Takt W in $v^{(s+1)} = \varphi(u^{(s)}, x^{(s)})$ übergeht, und Outputzeichen $y^{(s+1)} = \psi(v^{(s)}, x^{(s)})$ abgibt; A aber in $a^{(s+1)} = f(a^{(s)}, y^{(s+1)})$ übergeht, und im Falle $a^{(s+1)} \notin \tau$ Outputzeichen $x^{(s+1)} = g(a^{(s)}, y^{(s+1)})$ abgibt; gilt aber $a^{(s+1)} \in \tau$ so gibt A schon kein Outputzeichen ab, und das Verfahren – d.h. die Arbeit des Kompaktums K – abbricht.

A nennt man für W anwendbar, falls das Kompaktum K ihre Arbeit für jeden möglichen Anfangszustand $v_\alpha^{(0)} \in \mathfrak{V}_0 (\alpha \in \Gamma)$ in endlich (aber von α natürlich abhängend) vielen Schritten beendet. Dadurch gehört zu jedem Anfangszustand $v_\alpha^{(0)} \in \mathfrak{V}_0$ ein Endzustand $v_\alpha^{(t)}(A) \in \mathfrak{V}$. Der Algorithmus A in der betrachteten Anwendung W ergibt also eine Abbildung $\mathfrak{X}$ von $\mathfrak{V}_0$ in $\{v_\alpha^{(t)}(A) | \alpha \in \Gamma\}$. Da aber hinsichtlich der Auswertung (der numerischen Bedeutung) der Ergebnisse einiger Zustände von W gleichwertig werden können, bedeute $\mathfrak{V}_\alpha^{(t)}(A) \subset \mathfrak{V}$ die Menge der Zustände, die mit $v_\alpha^{(t)}(A)$ hinsichtlich des Ergebnisses gleichwertig betrachtet werden können. Den Algorithmus, der durch A in W erzeugt ist, charakterisiert man also mit der Abbildung Ψ von $\mathfrak{V}_0$ in $\{\mathfrak{V}_\alpha^{(t)}(A) | \alpha \in \Gamma\}$. Wir sagen nun, dass die Pseudo-Mealysche Siebentupel B $(\mathfrak{B}, Y, X, h, k, b_0, \tau^*)$ in W mit A äquivalenten Algorithmus realisiert, falls die Zusammenschaltung von B und W die Arbeit für jeden möglichen Anfangszustand $v_\alpha^{(0)} \in \mathfrak{V}_0$ in endlich vielen Schritten beendet, und $v_\alpha^{(t)}(B) \in \mathfrak{V}_\alpha^{(t)}(A) = \Psi(v_\alpha^{(0)})$ für jedes $\alpha \in \Gamma$ feststeht. Die Güte des Algorithmus A in W kann man nun aus verschiedenen Gesichtspunkten messen. Zu jedem $\alpha \in \Gamma$ gehört nämlich eine Taktenzahl $N(\alpha, A)$, u.zw. die Anzahl der Takten, welche das Kompaktum $K = A \rightleftarrows W$ schreitet von $(a_0, v_\alpha^{(0)})$ ausgehend, um die Arbeit zu beendigen. Die „Tschebyschewsche" Güte von A ist nämlich $\sup N(\alpha, A)$, die „statistische" Güte aber $E[N(\alpha, A)]$, wo die Wahrscheinlichkeitsdichte über $\mathfrak{V}_0$ angegeben betrachtet ist. Die Optimierung

des Algorithmus bedeutet also das Aufsuchen einer solchen Pseudomealyschen Siebentupel C, welche mit A in W äquivalent ist, und für welche die Güte in der Menge aller mit A äquivalenten Siebentupeln am besten ist. Die Lösung dieser Optimierungsaufgabe ist gar nicht einfach, da es einen Charakter hat, den man unter dem Namen „Versuch mit Automaten" zusammenfasst. Ein direkten Weg für die Lösung ist gar nicht bekannt, um so mehr, da man im Falle, wenn nur Ψ angegeben ist, auch die Existenz einer entsprechenden Siebentupel im allgemeinen nicht sichern kann. Wir konnten jedoch im Falle, wenn A und W endliche Automaten sind, einerseits obere Schränken für $\inf \sup N(\alpha, B)$ bezw. $\inf\limits_{\{B \equiv A\}} [\mathscr{E}\ N(\alpha, B)]$ angeben, andererseits, mit Hilfe dieser Schränken Algorithmen des Typs „Dynamische Programmierung" um die Aufsuchung den besten Algorithmus realisierender Siebentupel beschreiben. Die Forderung der Endlichkeit ist in praktischen Fällen immer erfüllt, jedoch die praktische Konstruktion von W und A, umsomehr die Optimierung von A in genug allgemein gefassten Problemenkreisen so schwer ist, dass man sie nur in manchen Fällen ganz explizit durchführen kann. Jedoch die exakte Fassung der Optimierung von numerischen Rechenprozessen konnte man bisher gar nicht erledigen; der obige Gedankengang bedeutet den ersten exakten Versuch. Mit einem solchen Modell konnten wir z.B. zeigen, dass man allgemein die Lösung eines linearen Gleichungssystems mit n Unbekannten nur mit Hilfe eines Algorithmus finden kann, der mindestens $O(n^3)$ Multiplikationen enthält. Ersetzt man den Pseude-Mealyschen determinierten Anfangsautomaten A mit einem stochastischen, so bekommt man Ergebnisse über beste Monte-Carlo-Methoden. Der wichtigste Schritt wird in dieser Theorie jedoch sein, wenn es uns gelingt, die Theorie der diskreten Automaten auf die stetigen zu übertragen. So bekommt man einerseits qualitative Informationen über die besten numerischen Algorithmen, anderseits gute Abschätzungen über den Operationsbedarf dieser Algorithmen.

Ich kehre jetzt zur informationstheoretischen Behandlung von Babuška und Sobolev dieses Problemenkreisses zurück. Die durch Ihnen angegebenen Ergebnisse waren sehr überraschend, jedoch eben in den einfachsten Fällen kann man keine genügende Abschätzungen bekommen (z.B. bekommt man dieselbe Abschätzung für die Anzahl der binären Entscheidungen bei der Bildung von Summen einerseits, von Produkten anderseits). Die Schwierigkeiten treten von zwei Seiten auf, welche wir bisher noch nicht bzw. nur teilweise lösen konnten. Einerseits kann man informationstheoretisch nicht beweisen, dass die Lösung einer gut charakterisierten Problemenschar in ε-Pünktlichkeit nie mit weniger binären Entscheidungen sich angeben lässt, als die ε-Entropie der kompakten Teilmenge des Raumes, wo die gesuchte Lösung der betrachteten Schar liegt. Anderseits probierte ich die ursprüngliche Idee so verfeinern, dass sie in den einfachsten Fällen die erwartete Abschätzungen ausgebe, was nur Teilweise gelang. Die folgende Ideen baute ich in die Theorie ein. Einerseits: In den praktischen Fällen findet bzw. sucht man nicht nur die Lösung, sondern auch die Eingangsdaten in einer kompakten Teilmenge eines entsprechenden linearen

supermetrischen Raumes. Man soll also den Raum, bzw. eine kompakte Teilmenge $\mathfrak{D}$ des Raumes der Eingangsdaten betrachten, und für diese das beste Netz $\mathfrak{N}(\varepsilon)$ – mit wenigsten Netzpunkten – angeben, welche die folgende Eigenschaft besitzt: zu jedem Netzpunkt $N \in \mathfrak{N}(\varepsilon)$ gibt es eine offene Teilmenge $\mathfrak{R}(N) \subset \mathfrak{D}$ derart, dass für jede Eingangsdatengruppe $d \in \mathfrak{R}(N)$ eine solche Lösung gehört, welche in ε-Pünktlichkeit mit der zu N gehörenden Lösung übereinstimmt, und $U\mathfrak{R}(N)$ die ganze $\mathfrak{D}$ überdeckt. Die Entropie dieses Netzes $\mathfrak{N}(\varepsilon)$ soll man als untere Schranke der minimalen Grundoperationsbedarf des besten Algorithmus betrachten. Man kann es folgendermassen plausibel machen: Hätten wir schon alle Aufgaben der betrachteten Problemenschar in ε-Pünktlichkeit gelöst, so brauchte man nur einen solchen Netzpunkt aus unserer Sammlung aussuchen, bei welchem die zugeordnete effene Teilmenge $\mathfrak{R}(N)$ die angegebenen Eingangsdaten enthält. Somit bekommt man eine Theorie, welche auch den Zusammenhang der Daten und Ergebnissen betrachtet, und zeigt einen charakteristischen Unterschied zwischen den linearen und nichtlinearen Problemen. Aber auch diese Idee scheint nür für direkte Problemenklassen entsprechend zu sein (wo also Operator und Operand angegeben ist, und Ergebnis gesucht wird). Für indirekte Problemenklassen (Operator und Ergebnis angegeben, Operand zu suchen ist) soll man die obige Entropie, wie binärische Entscheidungsarbeit für eine Entscheidung in der betrachteten kompakten Teilmenge des Raumes der Lösungen zu betrachten (d.h. Entscheidung dafür, ob das ausgewählte Element eine Lösung ist, oder nicht) und Entropie des ursprünglich durch Babuška und Sobolev angegebenen Modells mit der Entropie des oben angegebenen Modells zu multiplizieren. So bekommt man ein solches Mass für den Operationsbedarf, welches die erwartete Grössenordnung in den einfachsten Problemenscharen (Auflösung von linearen und nichtlinearen Gleichungssystemen, Spektraldarstellung von Matrizen, usw.) gut spiegelt. Jedoch auch so bekommt man keinen Unterschied zwischen Summenbildung und Produktbildung und es zeigt meiner Meinung nach, dass unser Modell noch immer nicht genügend ist.

Es bleibt noch die Frage: kann man den obigen Informationstheoretischen Gedankengang, bzw. Abschätzungen mit Hilfe der automatentheoretischen Überlegungen theoretisch streng begründen? In dieser Hinsicht haben wir die folgende Schwierigkeiten. Erstens: Bei der Konstruktion des Automaten, welcher den optimalen Algorithmus realisiert, braucht man eine möglichst gute obere Abschätzung für die Länge des längsten Eingabewortes, mit dessen Hilfe man die Abbildung Ψ in optimaler Weise in W realisiert; für die Begründung der Informationstheoretischen Betrachtungen braucht man aber eine möglichst gute untere Abschätzung für die Länge des kürzesten Eingabewortes, mit dessen Hilfe man die Abbildung Ψ für einen einzigen möglichen Anfangszustand $v_\alpha^{(0)} \in \mathfrak{V}_0$ realisiert. Es ist nun uns gelungen, auch in dieser Hinsicht gut brauchbare Abschätzungen angeben, um so mehr, mit Hilfe dieser Überlegungen auch den Konstruktionsalgorithmus des besten, die angegebene Abbildung Ψ zu realisierenden Automaten so verbessern, dass er jetz schon auch im Falle unendlicher Automaten theoretisch brauchbar ist.

Zweitens: Um die informationstheoretischen Überlegungen streng zu begründen, muss man die Problematik der besten Rechenprozessen ganz allgemein betrachten. In konkreten Fällen kann man den Kreis der erlaubten Grundoperationen durch die konkrete Angabe des Automaten W charakterisieren. Wie kann aber man es dann tun, wenn man das Problem ganz allgemein erfassen will, und alle algebraischen und logischen Elementaroperationen zu betrachten sind? Das ist uns folgendermassen gelungen: um die Brücke zwischen den diskreten und stetigen Automaten aufzubauen, haben wir eine Metrik für die Zustände eines Automaten eingeführt, undzwar eine erste Annäherung des Abstandes zweier Zustände mit Hilfe der Ausgabefunktion des Automaten, und dann mit Hilfe einer unendlichen Folge den Abstand selbst mit Hilfe der Durchgangsfunktion. Dieser Abstand ist nun dann und nur dann gleich 0, falls die Zustände einander äquivalent sind; die Grösse dieses Abstandes mässt nun die „Unäquivalenz" der betrachteten Zustände. Mit Hilfe dieses Abstandsbegriffes kann man nun die möglichen Operationen, durchgeführt durch den Anwendungsautomaten, so beschränken, dass man nur solche Eingangsbuchstaben zulässt, die eine solche Zustandsänderung bewirken können, welche eine angegebene Abstandsgrenze nicht überschreitet.

Drittens: Das Problem, warum die Lösung der Versuchsfragen bei diskreten Automaten schwer ist, steckt darin, dass man nur durch die Outputzeichen von W immer mehr Information über den momentanen Zustand sammeln kann. Je mächtiger also das Ausgangspalphabet des Anwendungsautomaten ist, desto kürzer kann das Versuchswort sein. Wie soll man also bei einer ganz allgemeinen Fassung des Operationsbedarfes von Algorithmen das Ausgangsalpahbet wählen? Es steht nahe, dass wir in jedem Schritt nur eine binärsche Entscheidung dh. ein zweilettriges Ausgangsalphabet in W zulassen.

Bei diesen Voraussetzungen konnten wir beweisen, dass die informationstheoretische Begründung des Operationsbedarfes von bestmöglichen Algorithmen — wie ich es früher skizziert habe — exakt ist.

Literaturverzeichnis

[1] *И. Бабушка-С. Л. Соболев:* Оптимизация численных методов. Apl. mat. *10*, 1965, 96—129.

[2] *Rutledge, J. D.:* On Janov's Program Schemata. Journal of the Assoc. for Comp. Machinery V.11. N.1. (1964) pp. 1—9.

[3] *Ginsburg, S.:* An Introduction to Mathematical Machine Theory. Addison — Wesley Publ. C. Reading, Palo Alto, London, 1962.

Prof. *Tamás Frey,* MTA Számítástechnikai Központja, Budapest I, Uri u. 49.