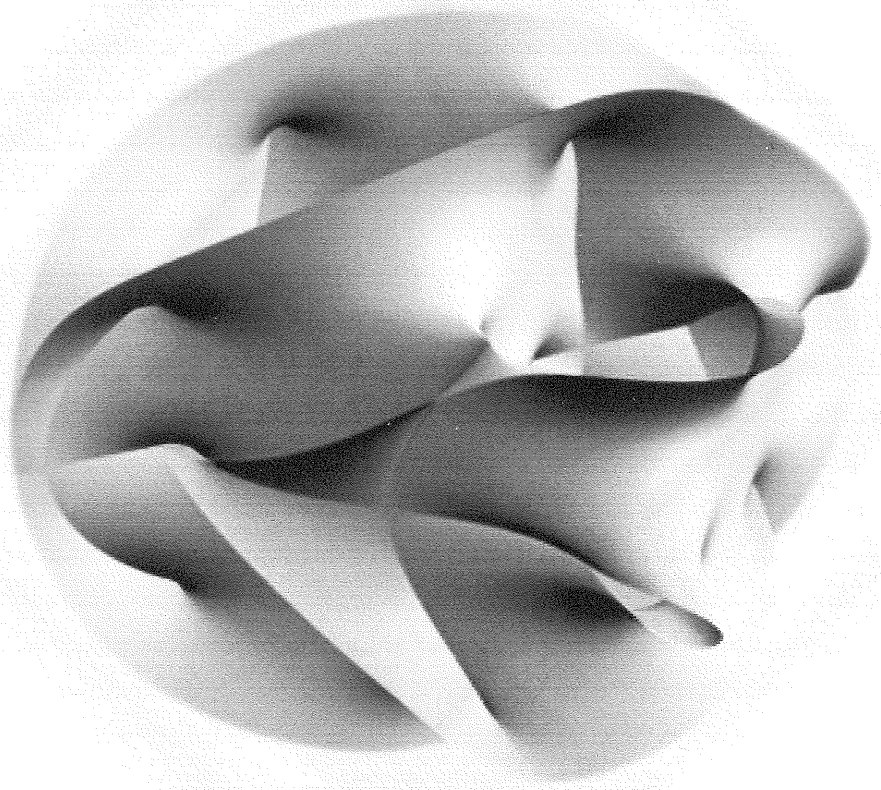
蛙鸣

第63期



中国科学技术大学数学系 编

2009年6月

刊首寄语

一处处清脆的蛙声，此起彼伏，奏响了夏的乐章。而沉甸甸的收获之美，也在这份轻快的欢悦中积蓄着，酝酿着。

翻开扉页，伴着淡淡书香，你可以在《蛙鸣》里聆听数学大家的睿语哲言，可以感悟身边师长们的求索历程，更可以采撷那转瞬即逝的思想的花瓣。在这里，青涩的推理将升华为一种灵动，稚嫩的笔迹将打磨成一种从容，思维的碎片将被拼接成一场精妙的演绎。

“当思维坠在灵魂上/如同露水坠在牧草上。”让我们铭记这些如同蛙鸣一般轻盈的自然原声吧！愿这期《蛙鸣》，能与你我的梦想共舞，在燥热的夏日里，呈上一份宁谧的思索。

目 录

大师睿语

特邀稿

研究探讨

蛙声一片

新生园地

WHAT IS GOOD MATHEMATICS?

TERENCE TAO

Abstract

Some personal thoughts and opinions on what "good quality mathematics" is, and whether one should try to define this term rigorously. As a case study, the story of Szemerédi's theorem is presented.

1.The many aspects of mathematical quality

We all agree that mathematicians should strive to produce good mathematics. But how does one define "good mathematics", and should one even dare to try at all? Let us first consider the former question. Almost immediately one realises that there are many different types of mathematics which could be designated "good". For instance, "good mathematics" could refer (in no particular order) to

(i) Good mathematical problem-solving (e.g. a major breakthrough on an important mathematical problem);

(ii) Good mathematical technique (e.g. a masterful use of existing methods, or the development of new tools);

(iii) Good mathematical theory (e.g. a conceptual framework or choice of notation which systematically unifies and generalises an existing body of results);

(iv) Good mathematical insight (e.g. a major conceptual simplification, or the realisation of a unifying principle, heuristic, analogy, or theme);

(v) Good mathematical discovery (e.g. the revelation of an unexpected and intriguing new mathematical phenomenon, connection, or counterexample);

(vi) Good mathematical application (e.g. to important problems in physics, engineering, computer science, statistics, etc., or from one field of mathematics to another);

(vii) Good mathematical exposition (e.g. a detailed and informative survey on a timely mathematical topic, or a clear and well-motivated argument);

(viii) Good mathematical pedagogy (e.g. a lecture or writing style which enables others to learn and do mathematics more effectively, or contributions to mathematical education);

(ix) Good mathematical vision (e.g. a long-range and fruitful program or set of conjectures);

(x) Good mathematical taste (e.g. a research goal which is inherently interesting and impacts important topics, themes, or questions);

(xi) Good mathematical public relations (e.g. an effective showcasing of a mathematical achievement to non-mathematicians, or from one field of mathematics to another);

(xii) Good meta-mathematics (e.g. advances in the foundations, philosophy, history, scholarship, or practice of mathematics);
(xiii) Rigorous mathematics (with all details correctly and carefully given in full);
(xiv) Beautiful mathematics (e.g. the amazing identities of Ramanujan; results which are easy (and pretty) to state but not to prove);
(xv) Elegant mathematics (e.g. Paul Erdós' concept of "proofs from the Book"; achieving a difficult result with a minimum of effort);
(xvi) Creative mathematics (e.g. a radically new and original technique, viewpoint, or species of result);
(xvii) Useful mathematics (e.g. a lemma or method which will be used repeatedly in future work on the subject);
(xviii) Strong mathematics (e.g. a sharp result that matches the known counterexamples, or a result which deduces an unexpectedly strong conclusion from a seemingly weak hypothesis);
(xix) Deep mathematics (e.g. a result which is manifestly non-trivial, for instance by capturing a subtle phenomenon beyond the reach of more elementary tools);
(xx) Intuitive mathematics (e.g. an argument which is natural and easily visualisable);
(xxi) Definitive mathematics (e.g. a classification of all objects of a certain type; the final word on a mathematical topic);
(xxii) etc., etc. [1]

As the above list demonstrates, the concept of mathematical quality is a high-dimensional one, and lacks an obvious canonical total ordering.[2] I believe this is because mathematics is itself complex and high-dimensional, and evolves in unexpected and adaptive ways; each of the above qualities represents a different way in which we as a community improve our understanding and usage of the subject. There does not appear to be universal agreement as to the relative importance or weight of each of the above qualities. This is partly due to tactical considerations: a field of mathematics at a given stage of development may be more receptive to one approach to mathematics than another. It is also partly due to cultural considerations: any given field or school of mathematics tends to attract like-minded mathematicians who prefer similar approaches to a subject. It also reflects the diversity of mathematical ability; different mathematicians tend to excel in different mathematical styles, and are thus well suited for different types of mathematical challenges. (See also [12] for some related discussion.)

I believe that this diverse and multifaceted nature of "good mathematics" is very healthy for mathematics as a whole, as it it allows us to pursue many different approaches to the subject, and exploit many different types of mathematical talent, towards our common goal of greater mathematical progress and understanding. While each one of the above attributes is generally accepted to be a desirable trait to have in mathematics, it can become detrimental to a field

[1] The above list is not meant to be exhaustive. In particular, it focuses primarily on the type of mathematics found in mathematical research papers, as opposed to classrooms, textbooks, or papers in disciplines close to mathematics, such as the natural sciences.

[2] In particular, it is worth pointing out that mathematical rigour, while highly important, is only one component of what determines a quality piece of mathematics.

Mathematics is the most beautiful and most powerful creation of the human spirit.
— — Stefan Banach

to pursue only one or two of them at the expense of all the others. Consider for instance the following hypothetical (and somewhat exaggerated) scenarios:

- A field which becomes increasingly ornate and baroque, in which individual results are generalised and refined for their own sake, but the subject as a whole drifts aimlessly without any definite direction or sense of progress;
- A field which becomes filled with many astounding conjectures, but with no hope of rigorous progress on any of them;
- A field which now consists primarily of using ad hoc methods to solve a collection of unrelated problems, which have no unifying theme, connections, or purpose;
- A field which has become overly dry and theoretical, continually recasting and unifying previous results in increasingly technical formal frameworks, but not generating any exciting new breakthroughs as a consequence; or
- A field which reveres classical results, and continually presents shorter, simpler, and more elegant proofs of these results, but which does not generate any truly original and new results beyond the classical literature.

In each of these cases, the field of mathematics exhibits much activity and progress in the short term, but risks a decline of relevance and a failure to attract younger mathematicians to the subject in the longer term. Fortunately, it is hard for a field to stagnate in this manner when it is constantly being challenged and revitalised by its connections to other fields of mathematics (or to related sciences), and by exposure to (and respect for) multiple cultures of "good mathematics". These self-correcting mechanisms help to keep mathematics balanced, unified, productive, and vibrant.

Let us turn now to the other question posed above, namely whether we should try to pin down a definition of "good mathematics" at all. In doing so, we run the risk of arrogance and hubris; in particular, we might fail to recognise exotic examples of genuine mathematical progress because they fall outside mainstream definitions[3] of "good mathematics". On the other hand, there is a risk also in the opposite position - that all approaches to mathematics are equally suitable and deserving of equal resources[4] for any given mathematical field of study, or that all contributions to mathematics are equally important; such positions may be admirable for their idealism, but they sap mathematics of its sense of direction and purpose, and can also lead to a sub-optimal allocation of mathematical resources[5]. The true situation lies somewhere in between; for each area of mathematics, the existing body of results, folklore, intuition and experience (or lack thereof) will indicate which types of approaches are likely to be fruitful and thus deserve the majority of resources, and which ones are more speculative and which

[3] A related difficulty is that, with the notable exception of mathematical rigour, most of the above qualities are somewhat subjective, and contain some inherent imprecision or uncertainty. We thank Gil Kalai for emphasising this point.

[4] Examples of scarce resources include money, time, attention, talent, and pages in top journals.

[5] Another solution to this problem is to exploit the fact that mathematical resources are also high- dimensional, for instance one can award prizes for exposition, for creativity, etc., or have different journals devoted to different types of achievement. We thank Gil Kalai for this observation.

might warrant inspection by only a handful of independently minded mathematicians, just to cover all bases. For example, in mature and well-developed fields, it may make sense to pursue systematic programs and develop general theories in a rigorous manner, conservatively following tried-and-true methods and established intuition, whereas in newer and less settled fields, a greater emphasis might be placed on making and solving conjectures, experimenting with different approaches, and relying to some extent on non-rigorous heuristics and analogies. It thus makes sense from a tactical point of view to have at least a partial (but evolving) consensus within each field as to what qualities of mathematical progress one should prize the most, so that one can develop and advance the field as effectively as possible at each stage of its development. For instance, one field may be in great need of solutions to pressing problems; another field may be crying out for a theoretical framework to organise the clutter of existing results, or a grand program or series of conjectures to stimulate new results; other fields would greatly benefit from new, simpler, and more conceptual proofs of key theorems; yet more fields may require good publicity, and lucid introductions to the subject, in order to attract more activity and interest. Thus the determination of what would constitute good mathematics for a field can and should depend highly on the state of the field itself. It should also be a determination which is continually updated and debated, both within a field and by external observers to that field; as mentioned earlier, it is quite possible for a consensus on how a field should progress to lead to imbalances within that field, if they are not detected and corrected in time.

It may seem from the above discussion that the problem of evaluating mathematical quality, while important, is a hopelessly complicated one, especially since many good mathematical achievements may score highly on some of the qualities listed above but not on others; also, many of these qualities are subjective and difficult to measure precisely except with hindsight. However, there is the remarkable phenomenon[6] that good mathematics in one of the above senses tends to beget more good mathematics in many of the other senses as well, leading to the tentative conjecture that perhaps there is, after all, a universal notion of good quality mathematics, and all the specific metrics listed above represent different routes to uncover new mathematics, or different stages or aspects of the evolution of a mathematical story.

2.Case study: Szemerédi's theorem

Turning now from the general to the specific, let us now illustrate the phenomenon mentioned in the preceding paragraph by considering the history and context of Szemerédi's theorem [32] - the beautiful and celebrated result that any subset of integers of positive (upper) density must necessarily contain arbitrarily long arithmetic progressions. I will avoid all technical details here; the interested reader is referred to [33] and the references therein for further discussion.

[6]This phenomenon is also somewhat related to the "unreasonable effectiveness of mathematics" observed by Wigner [38].

It is easier to square the circle than to get round a mathematician.

— — Augustus de Morgan

There are several natural places to start this story. I will begin with Ramsey's theorem [23]: that any finitely coloured, sufficiently large complete graph will contain large monochromatic complete subgraphs. (For instance, given any six people, either three will know each other, or three will be strangers to each other, assuming of course that "knowing one another" is a well-defined and symmetric relation.) This result, while simple to prove (relying on nothing more than an iterated pigeonhole principle), represented the discovery of a new phenomenon and created a new species of mathematical result: the Ramsey-type theorem, each one of which being a different formalisation of the newly gained insight in mathematics that complete disorder is impossible.

One of the first Ramsey-type theorems (which actually predates Ramsey's theorem by a few years) was van der Waerden's theorem [37]: given any finite colouring of the integers, one of the colour classes must contain arbitrarily long arithmetic progressions. Van der Waerden's highly recursive proof was very elegant, but had the drawback that it offered fantastically poor quantitative bounds for the appearance of the first arithmetic progression of a given length; indeed, the bound involved an Ackermann function of this length and the number of colours. Erdós and Turán [4] had the good mathematical taste to pursue this quantitative question [7] further, being motivated also by the desire to make progress on the (then conjectural) problem of whether the primes contained arbitrarily long progressions. They then advanced a number of strong conjectures, one of which became Szemerédi's theorem; another was the beautiful but (still open) stronger statement that any set of positive integers whose reciprocals were not absolutely summable contained arbitrarily long arithmetic progressions.

The first progress on these conjectures was a sequence of counterexamples, culminating in the elegant construction of Behrend [1] of a moderately sparse set (whose density in 1, . . . ,N was asymptotically greater than N-" for any fixed ") without arithmetic progressions of length three. This construction ruled out the most ambitious of the Erdós-Turán conjectures (in which polynomially sparse sets were conjectured to have many progressions), and as a consequence also ruled out a significant class of elementary approaches to these problems (e.g. those based on inequalities such as the Cauchy-Schwarz or Hölder inequalities). While these examples did not fully settle the problem, they did indicate that the Erdós-Turán conjectures, if true, would necessarily have a non-trivial (and thus presumably interesting) proof.

The next major advance was by Roth [27], who applied the Hardy-Littlewood circle method[8] together with a new method (the density increment argument) in a beautifully elegant manner to establish Roth's theorem: every set of integers of positive density contained infinitely many progressions of length three. It was then natural to try to extend Roth's methods to progressions of longer length. Roth and many others tried to do so for many years,

[7] Erdós also pursued the question of quantitative bounds for the original theorem of Ramsey, leading among other things to the founding of the immensely important probabilistic method in combinatorics, but this is a whole story in itself which we have no space to discuss here.

[8] Again, the history of the circle method is another great story which we cannot detail here. Suffice to say though that this method, in modern language, is part of the now standard insight that Fourier analysis is an important tool for tackling problems in additive combinatorics.

数学之所以比一切其它科学受到尊重，一个理由是因为他的命题是绝对可靠和无可争辩的，而其它的科学经常处于被新发现的事实推翻的危险。数学之所以有高声誉，另一个理由就是数学使得自然科学实现定理化，给予自然科学某种程度的可靠性。

——爱因斯坦

but without full success; the reason for the obstruction here was not fully appreciated until the work of Gowers much later. It took the formidable genius of Endré Szemerédi [31], [32], who returned to purely combinatorial methods (in particular, pushing the density increment argument to remarkable new levels of technical sophistication) to extend Roth's theorem first to progressions of length four[9], and then to progressions of arbitrary length, thus establishing his famous theorem. Szemerédi's proof was a technical tour de force, and introduced many new ideas and techniques, the most important of which was a new way to look at extremely large graphs, namely to approximate them by bounded complexity models. This result, the celebrated and very useful Szemerédi regularity lemma, is notable on many levels. As mentioned above, it gave a radically new insight regarding the structure of large graphs (which in modern language is now regarded as a structure theorem as well as a compactness theorem for such graphs); it gave a new proof method (the energy increment method) which will become crucial later in this story; and it also generated an incredibly large number of unexpected applications, from graph theory to property testing to additive combinatorics; the full story of this regularity lemma is unfortunately too lengthy to be described here.

While Szemerédi's accomplishment is undoubtedly a highlight of this particular story, it was by no means the last word on the matter. Szemerédi's proof of his theorem, while elementary, was remarkably intricate, and not easily comprehended. It also did not fully resolve the original questions motivating Erdós and Turán, as the proof itself used van der Waerden's theorem at two key junctures and so did not give any improved quantitative bound on that theorem. Furstenberg then had the mathematical taste to seek out a radically different (and highly non-elementary[10]) proof, based on an insightful analogy between combinatorial number theory and ergodic theory which he soon formalised as the very useful Furstenberg correspondence principle. From this principle[11] one readily concludes that Szemerédi's theorem is equivalent to a multiple recurrence theorem for measure-preserving systems. It then became natural to prove this theorem (now known as the Furstenberg recurrence theorem) directly by methods from ergodic theory, in particular by exploiting the various classifications and structural decompositions (e.g. the ergodic decomposition) available for such systems. Indeed, Furstenberg soon established the Furstenberg structure theorem, which described any measure preserving system as a weakly mixing extension of a tower of compact extensions of a trivial system, and based on this theorem and several additional arguments (including a variant of the van der Waerden argument) was able to establish the multiple recurrence theorem, and thus give a new proof of Szemerédi's theorem. It is also worth mentioning that Furstenberg also produced an excellent book [6] on this and related topics, which systematically formalised the basic theory while also

[9]Shortly afterward, Roth [28] was able to combine some of Szemerédi' s ideas with his own Fourier analytic method to create a hybrid proof of Szemer' edi' s theorem for progressions of length four.

[10]For instance, some versions of Furstenberg' s argument rely heavily on the axiom of choice, though it is possible to also recast the argument in a choice-free manner.

[11]There is also a similar correspondence principle which identifies van der Waerden's theorem with a multiple recurrence theorem for topological dynamical systems. This leads to the fascinating story of topological dynamics, which we unfortunately have no space to describe here.

A computer would deserve to be called intelligent if it could deceive a human into believing that it was human.

— — Alan Turing

contributing greatly to the growth and further development of this area.

Furstenberg and his coauthors then realised that this new method was potentially very powerful, and could be used to establish many more types of recurrence theorems, which (via the correspondence principle) then would yield a number of highly non-trivial combinatorial theorems. Pursuing this vision, Furstenberg, Katznelson, and others obtained many variants and generalisations of Szemerédi's theorem, obtaining for instance variants in higher dimensions and even establishing a density version of the Hales-Jewett theorem [18] (a very powerful and abstract generalisation of the van der Waerden theorem). Many of the results obtained by these infinitary ergodic theory techniques are not known, even today, to have any "elementary" proof, thus testifying to the power of this method. Furthermore, as a valuable byproduct of these efforts, a much deeper understanding of the structural classification of measure-preserving systems was obtained. In particular, it was realised that for many classes of recurrence problem, the asymptotic recurrence properties of an arbitrary system are almost completely controlled by a special factor of that system, known as the (minimal) characteristic factor of that system[12]. Determining the precise nature of this characteristic factor for various types of recurrence then became a major focus of study, as it was realised that this would lead to more precise information on the limiting behaviour (in particular, it would show that certain asymptotic expressions related to multiple recurrence actually converged to a limit, which was a question left open from Furstenberg's original arguments). Counterexamples of Furstenberg and Weiss, as well as results of Conze and Lesigne, eventually led to the conclusion that these characteristic factors should be describable by a very special (and algebraic) type of measure-preserving system, namely a nilsystem associated with nilpotent groups; these conclusions culminated in precise and rigorous descriptions of these factors in a technically impressive paper of Host and Kra [20] (and subsequently also by Ziegler [39]), which among other things settled the question mentioned earlier concerning convergence of the asymptotic multiple recurrence averages. The central role of these characteristic factors illustrated quite starkly the presence of a dichotomy between structure (as represented here by nilsystems), and randomness (which is captured by a certain technical type of "mixing" property), and to the insight that it is this dichotomy which in fact underlies and powers Szemerédi' s theorem and its relatives. Another feature of the Host-Kra analysis worth mentioning is the prominent appearance of averages associated to "cubes" or "parallelopipeds", which turn out to be more tractable to analyse for a number of reasons than the multiple recurrence averages associated to arithmetic progressions.

In parallel to these ergodic theory developments, other mathematicians were seeking to understand, reprove, and improve upon Szemerédi's theorem in other ways. An important conceptual breakthrough was made by Ruzsa and Szemerédi [29], who used the Szemerédi regularity lemma mentioned earlier to establish a number of results in graph theory, including what is now known as the triangle removal lemma, which roughly asserts that a graph which contains a small number triangles can have those triangles removed by deleting a surprisingly

[12] An early example of this is von Neumann' s mean ergodic theorem, in which the factor of shift- invariant functions controls the limiting behaviour of simple averages of shifts.

small number of edges. They then observed that the Behrend example mentioned earlier gave some limits as to the quantitative bounds in this lemma, in particular ruling out many classes of elementary approaches to this lemma (as such approaches typically give polynomial type bounds); indeed to this day all known proofs of the removal lemma proceed via some variant of the regularity lemma. Applying this connection in the contrapositive, it was observed that in fact the triangle removal lemma implied Roth's theorem on progressions of length three. This discovery opened up for the first time the possibility that Szemerédi type theorems could be proven by purely graph-theoretical techniques, discarding almost entirely the additive structure of the problem. (Note that the ergodic theory approach still retained this structure, in the guise of the action of the shift operator on the system; also, Szemerédi's original proof is only partly graph-theoretical, as it exploits the additive structure of progressions in many different places.) It took some time though to realise that the graph theoretic method, like the Fourier-analytic method before it, was largely restricted to detecting "low complexity" patterns such as triangles or progressions of length three, and to detect progressions of longer length would require the substantially more difficult theory of hypergraphs. In particular this motivated the program (spearheaded by Frankl and Rödl) for obtaining satisfactory analogue of the regularity lemma for hypergraphs, which would be strong enough to yield consequences such as Szemerédi's theorem (as well as a number of variants and generalisations). This turned out to be a surprisingly delicate task, in particular carefully arranging the hierarchy[13] of parameters involved in such a regularisation so that they dominated each other in the correct order. Indeed the final versions of the regularity lemma, and the companion "counting lemmas" from which one could deduce Szemerédi's theorem, have only appeared rather recently ([22], [24], [25], [26], [14], . . .). It is also worth mentioning a very instructive counterexample [10] of Gowers, which shows that the quantitative bounds in the original regularity lemma must be at least tower-exponential in nature, thus indicating again the non-trivial nature (and power) of this lemma.

The Fourier analytic approach to Szemerédi's theorem, which had not progressed significantly since the work of Roth, was finally revisited by Gowers [11], [13]. As with other approaches, the Fourier-analytic approach proceeded by establishing a dichotomy on sets of integers, that they were either structured or pseudorandom in some sense. The relevant notion of structure here was worked out by Roth - structured sets should enjoy a density increment on medium-length arithmetic progressions - but the correct notion of pseudorandomness or "uniformity" was less clear. Gowers produced an example (closely related, in fact, to examples of Furstenberg and Weiss mentioned earlier) showing that Fourier-based notions of pseudorandomness were inadequate for controlling progressions of length four and higher, and then proceeded to introduce a different notion of uniformity (very closely related to the cube averages of Host and Kra, and also to certain notions of hypergraph regularity) which sufficed. The remaining task was to establish a quantitative and rigorous form of the dichotomy. This

[13]This hierarchy seems related to the towers of extensions encountered by Furstenberg in his anal- ogous quest to "regularise" a measure-preserving system, though the precise connection is still poorly understood at present.

A mathematical theory is not to be considered complete until you have made it so clear that you can explain it to the first man whom you meet on the street.
—— David Hilbert

turned out to be surprisingly difficult (mainly due to the limited utility of the Fourier transform in this setting), and in many ways analogous to the efforts of Host-Kra and Ziegler to endow characteristic factors with the algebraic structure of nilsystems. However, by combining Fourier analytic tools with major results from additive combinatorics such as Freiman's theorem and the Balog-Szemerédi theorem (the history of these being also an interesting story in its own right, see e.g. [35]), together with several new combinatorial and probabilistic methods, Gowers was able to achieve this in a remarkable tour de force, and in particular obtained remarkably strong quantitative bounds on Szemerédi's theorem and van der Waerden's theorem[14].

To summarise so far, four parallel proofs of Szemerédi's theorem have been achieved; one by direct combinatorics, one by ergodic theory, one by hypergraph theory, and one by Fourier analysis and additive combinatorics. Even with so many proofs, there was still a sense that our understanding of this result was still incomplete; for instance, none of the approaches were powerful enough to detect progressions in the primes, mainly because of the sparsity of the prime sequence. (The Fourier method, or more precisely the Hardy-Littlewood-Vinogradov circle method, can be used however to establish infinitely many progressions of length three in the primes [36], and with substantially more effort can also partially address progressions of length four [19].) However, by using ideas from restriction theory in harmonic analysis (which is another fascinating story that we will not discuss here), Green [15] was able to treat the primes "as if" they were dense, and in particular obtain an analogue of Roth' s theorem for dense subsets of primes. This opened up the intruiging possibility of a relative Szemerédi theorem, allowing one to detect arithmetic progressions in dense subsets of other sets than the integers, for instance dense subsets of primes. Indeed, a prototypical relative Roth theorem for dense subsets of quite sparse random sets had already appeared in the graph theory literature [21].

In joint work[15] with Ben Green, we began the task of trying to relativise Gowers ourier analytic and combinatorial arguments to such contexts as dense subsets of sparse random or "pseudorandom" sets. After much effort (inspired in part by the hypergraph theory, which was well adapted to count patterns in sparse sets, and also in part by an "arithmetic regularity lemma" of Green [16] that adapted the regularity lemma ideas from graph theory to additive contexts) we were eventually able (in an unpublished work) to detect progressions of length four in such sets. At this point we realised the analogies between the regularity lemma approach we were using, and the characteristic factor constructions in Host-Kra, and by substituting[16] in those constructions (in particular relying heavily on cube averages) we were able to establish a

[14]It is worth noting also the brilliantly creative proof of van der Waerden's theorem by Shelah [30], which held the previous record for the best constants for this theorem; the ideas of Shelah's proof have not yet been successfully integrated into the rest of the subject, but I expect that this will happen in the future.

[15]Incidentally, I was initially attracted to these problems by their intersection with another great mathematical story, that of the Kakeya conjecture, which we again do not have space to discuss here. It is however related in a somewhat surprising fashion with the story of restriction theory mentioned earlier.

[16]This was a little tricky for a number of reasons, most notably that the ergodic theory constructions were infinitary in nature, whereas to deal with the primes it was necessary to work in a finitary context. Fortunately I had already attempted to finitise the ergodic approach to Szemer′ edi' s theorem [34]; while that attempt was incomplete at the time, it turned out to have enough substance to be helpful for the application to the primes.

satisfactory relative Szemerédi theorem, which relied on a certain transference principle which asserted, roughly speaking, that dense subsets of sparse pseudorandom sets behaved "as if" they were dense in the original space. In order to apply this theorem to the primes, we needed to enclose the primes in a suitably pseudorandom set (or more precisely a measure); but very fortuitiously for us, the recent breakthroughs[17] of Goldston and Yildidirm [8] on prime gaps[18] had constructed almost exactly what we needed for this purpose, allowing us to establish at last the old conjecture that the primes contained arbitrarily long arithmetic progressions.

The story still does not end here, but instead continues to develop in several directions. On one hand there are now a number of further applications of the transference principle, for instance to obtain constellations in the Gaussian primes or polynomial progressions in the rational primes. Another promising avenue of research is the convergence of the Fourier, hypergraph, and ergodic theory methods to each other, for instance in developing infinitary versions of the graph and hypergraph theory (which have applications to other areas of mathematics as well, such as property testing) or finitary versions of the ergodic theory. A third direction is to make the nilsystems that control recurrence in the ergodic theory setting, also control various finitary averages relating to arithmetic progressions; in particular, Green and I are actively working on computing correlations between primes and sequences generated by nilsystems (using methods dating back to Vinogradov) in order to establish more precise asymptotics on various patterns that can be found in the primes. Last, but not least, there is the original Erdós-Turán conjecture, which still remains open after all this progress, though there is now some very promising advances of Bourgain [2], [3] which should lead to further developments.

3. Conclusion

As we can see from the above case study, the very best examples of good mathematics do not merely fulfil one or more of the criteria of mathematical quality listed at the beginning of this article, but are more importantly part of a greater mathematical story, which then unfurls to generate many further pieces of good mathematics of many different types. Indeed, one can view the history of entire fields of mathematics as being primarily generated by a handful of these great stories, their evolution through time, and their interaction with each other. I would thus conclude that good mathematics is not merely measured by one or more of the "local" qualities listed previously (though these are certainly important, and worth pursuing and debating), but also depends on the more "global" question of how it fits in with other pieces of good mathematics, either by building upon earlier achievements or encouraging the development of future breakthroughs. Of course, without the benefit of hindsight it is difficult

[17] At the time of our paper, the construction we used was from a paper of Goldston and Yildirim that was retracted for an unrelated error, which they eventually repaired with some clever new ideas from Pintz [9]. This supports a point made earlier, that it is not absolutely necessary for a piece of mathematics to be absolutely correct in every detail in order to be of value to future (rigorous) work.

[18] Once again, the story of prime gaps is an interesting one which we will be unable to pursue here.

Everyone knows what a curve is, until he has studied enough mathematics to become confused through the countless number of possible exceptions.

—— Felix Klein

to predict with certainty what types of mathematics will have such a property. There does however seem to be some undefinable sense that a certain piece of mathematics is "on to something", that it is a piece of a larger puzzle waiting to be explored further. And it seems to me that it is the pursuit of such intangible promises of future potential are least as important an aspect of mathematical progress than the more concrete and obvious aspects of mathematical quality listed previously. Thus I believe that good mathematics is more than simply the process of solving problems, building theories, and making arguments shorter, stronger, clearer, more elegant, or more rigorous, though these are of course all admirable goals; while achieving all of these tasks (and debating which ones should have higher priority within any given field), we should also be aware of any possible larger context that one's results could be placed in, as this may well lead to the greatest long-term benefit for the result, for the field, and for mathematics as a whole.

4. Acknowledgements

I thank Laura Kim for reading and commenting on an early draft of this manuscript, and Gil Kalai for many thoughtful comments and suggestions

References

[1] F. A. Behrend, On sets of integers which contain no three terms in arithmetic progression, Proc. Nat. Acad. Sci. 32 (1946), 331-332.

[2] J. Bourgain, On triples in arithmetic progression, Geom. Func. Anal., 9 (1999), 968-984.

[3] J. Bourgain, Roth's theorem on arithmetic progressions revisited, preprint.

[4] P. Erdós, P. Turán, On some sequences of integers, J. London Math. Soc. 11 (1936), 261-264.

[5] H. Furstenberg, Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions, J. Analyse Math. 31 (1977), 204-256.

[6] H. Furstenberg, Recurrence in Ergodic theory and Combinatorial Number Theory, Princeton University Press, Princeton NJ 1981.

[7] H. Furstenberg, Y. Katznelson, D. Ornstein, The ergodic theoretical proof of Szemerédi's theorem, Bull. Amer. Math. Soc. 7 (1982), 527-552.

[8] D. Goldston, C. Yildirim, Small gaps between primes, I, preprint.

[9] D. A. Goldston, J. Pintz, and C.Y. Yildirim, Small gaps between primes II, preprint.

[10] T. Gowers, Lower bounds of tower type for Szemerédi's uniformity lemma, Geom. Func. Anal. 7 (1997), 322-337.

[11] T.Gowers, A new proof of Szemerédi's theorem for arithmetic progressions of length four, Geom. Func. Anal. 8 (1998), 529-551.

[12] T. Gowers, The two cultures of mathematics, in: Mathematics: Frontiers and Perspectives, International Mathematical Union. V. Arnold, M. Atiyah, P. Lax, B. Mazur, Editors. American Mathematical Society, 2000.

[13] T. Gowers, A new proof of Szemerédi's theorem, Geom. Func. Anal. 11 (2001), 465-588.
[14] T. Gowers, Quasirandomness, counting and regularity for 3-uniform hypergraphs, Combin. Probab. Comput. 15 (2006), no. 1-2, 143-184.
[15] B.J. Green, Roth's theorem in the primes, . Math. 161 (2005), 1609-1636.
[16] B.J. Green, A Szemerédi-type regularity lemma in abelian groups, Geom. Func. Anal. 15 (2005), no. 2, 340-376.
[17] B.J.Green, T. Tao, The primes contain arbitrarily long arithmetic progressions, to appear, Ann. Math.
[18] A.W. Hales, R.I.Jewett, Regularity and positional games, Trans. Amer. Math. Soc. 106 (1963), 222-229.
[19] D.R. Heath-Brown, Three primes and an almost prime in arithmetic progression, J. London Math. Soc. (2) 23 (1981), 396-414.
[20] B. Host, B. Kra, Non-conventional ergodic averages and nilmanifolds, Annals of Math. 161 (2005), 397-488.
[21] Y.Kohayakawa, T. Luczak, V. Rödl, Arithmetic progressions of length three in subsets of a random set, Acta Arith. 75 (1996), no. 2, 133-163.
[22] B. Nagle, V. Rödl, M. Schacht, The counting lemma for regular k-uniform hypergraphs, preprint.
[23] F. P. Ramsey, On a problem of formal logic, Proc. London Math. Soc. 30 (1930), 264-285.
[24] V. Rödl, M. Schacht, Regular partitions of hypergraphs, preprint.
[25] V. Rödl, J. Skokan, Regularity lemma for k-uniform hypergraphs, Random Structures and Algo- rithms, 25 (2004), no. 1, 1-42.
[26] V. Rödl, J. Skokan, Applications of the regularity lemma for uniform hypergraphs, Random Struc- tures and Algorithms, 28 (2006), no. 2, 180-194.
[27] K.F. Roth, On certain sets of integers, J. London Math. Soc. 28 (1953), 245-252.
[28] K.F. Roth, Irregularities of sequences relative to arithmetic progressions, IV. Period. Math. Hun- gar. 2 (1972), 301-326.
[29] I. Ruzsa, E. Szemerédi, Triple systems with no six points carrying three triangles, Colloq. Math. Soc. J. Bolyai 18 (1978), 939-945.
[30] S. Shelah, Primitive recursive bounds for van der Waerden numbers, J . Amer. Math. Soc. 1 (1988), 683-697.
[31] E. Szemerédi, On sets of integers containing no four elements in arithmetic progression, Acta Math. Acad. Sci. Hungar. 20 (1969), 89-104.
[32] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, Acta Arith. 27 (1975), 299-345.
[33] T. Tao, The dichotomy between structure and randomness, arithmetic progressions, and the primes, to appear, ICM 2006 proceedings.
[34] T. Tao, A quantitative ergodic theory proof of Szemerédi's theorem, preprint. [35] T. Tao and V. Vu, Additive Combinatorics, Cambridge Univ. Press, 2006.
[36] J.G. van der Corput, Über Summen von Primzahlen und Primzahlquadraten, Math. Ann.

I am interested in mathematics only as a creative art.

—— G. H. Hardy

116 (1939), 1-50.
[37] B. L. van der Waerden, Beweis einer Baudetschen Vermutung, Nieuw. Arch. Wisk. 15 (1927), 212-216.
[38] E. Wigner, The Unreasonable Effectiveness of Mathematics in the Natural Sciences, Comm. Pure Appl. Math. 13 (1960).
[39] T. Ziegler, Universal characteristic factors and Furstenberg averages, J. Amer. Math. Soc. 20 (2007), 53-97.

Department of Mathematics, UCLA, Los Angeles CA 90095-1555, USA.
E-mail address: tao@math.ucla.edu

陶哲轩简介

陶哲轩，英语名Terence Tao，小名Terry，生于澳大利亚阿德莱德，是华裔澳大利亚籍数学家，主要研究调和分析、偏微分方程、组合数学、解析数论和表示论。

他在小小年纪时便展现出数学天分。陶哲轩7岁进入高中，9岁进入大学，10岁、11岁、12岁参加国际数学奥林匹克竞赛分获铜牌、银牌、金牌，16岁获得学士学位，17岁获得硕士学位，21岁获得普林斯顿大学博士学位。从1992年至1996年，他是普林斯顿大学的研究生，指导教授是埃利亚斯·施泰因（Elias Stein）。

24岁时，他在加利福尼亚大学洛杉矶分校担任教授。他现在为该校终身数学教授。在1986年，1987年和1988年，陶哲轩是国际数学奥林匹克最年轻的参赛者，依次赢得铜牌、银牌和金牌。他未到13岁已赢得金牌，这项纪录至今无人打破。

他在2000年获颁塞勒姆奖，2002年获颁博谢纪念奖，和在2003年获颁克雷研究奖，以表扬他对分析学的贡献，当中包括挂谷猜想和wave map。在2005年，他获得利瓦伊·L·科南特奖（获奖者还有艾伦·克努森）。

在2004年，本·格林和陶哲轩发表了一篇论文预印稿，宣称证明存在任意长的素数等差数列。

2006年8月22日，他在西班牙马德里的国际数学家大会获得菲尔兹奖。并于2006年8月23日在国际数学家大会做了一小时报告。

◇◇

数学中的一些美丽定理具有这样的特性：它们极易从事实中归纳出来，但证明却隐藏的极深。

—— 高斯

对数学系主任陈发来老师的访谈

*05001*杨熠　整理

自从科大数学系从理学院独立出来，成为学校的一个直属系后，大家对数学系的发展有了更多的期待。很多同学十分关心数学系未来的学科建设方向和团队发展问题。带着这些来自同学们的心声，我们有幸在一个阳光明媚的下午同数学系主任陈发来老师进行了一次愉快的交流。

笔者：陈老师您好！首先非常感谢您在百忙之中接受我们的这次采访。这次主要想向您请教一些同学们平时比较关心的有关数学系建设的一些问题。首先想请问陈老师，数学系目前的课程设置是基于什么样的一个准则呢，今后是否将考虑做一些改变，比如增加数学课的数量和种类。

陈老师：是这样的，科大数学系的课程体系秉承了七、八十年代的特点，在经历了从5年制转变成为4年制，教育部规定的专业合并的改变，比如将基础与应用数学合二为一后，整个体系变化不是太大。我们的课程选择一向基于“重视基础，淡化专业”这八个字，力求让同学们在本科阶段为未来的发展储备坚实的基础。同时，希望同学们能够了解现今数学各个分支相互融合这个趋势，很多现在著名的数学家都在一定程度上是“通才”，比如陶哲轩。因此，相信“淡化专业”这个指导方针将有助于大家今后的成功。在对教学过程的观察中，我们也发现了一些课程教学的问题，而不是体系本身的问题。例如，很多同学对将基础与应用合为一个专业感到不适应。这个设置的确有一定的不合理性，比如对那些立志做应用数学研究的同学，一些很纯的数学课对他们今后的帮助性其实并不大。所以，现在我们数学系的课程被分为了以下四个部分：通识课（如物理类的课程），学科群基础课（如数学分析），专业必修课与专业选修课。其中我们的学科群基础课的课程数目在全国来看是最多最全的，这能在一定程度上让大家为今后的多方向工作研究做好准备。在专业必修课程的设置中，基础与应用的课程被分开了，这样能分别照顾学基础与学应用的同学。至于数学课的数量，目前由于师资原因，暂时开设的方向有限，我们将考虑今后引进多方面的人才，如优化、控制论方向的人才，争取能建立多方向的、全面的数学学科，满足同学们多方向的兴趣选择。

笔者：很感谢老师们为我们做的这些考虑。说到课程就不得不说说教材了。我听说，现在07级使用的实变函数的教材有变化。想请问陈老师，像这样换教材算是一个大的举动么？您对这个怎么看呢？

陈老师：数学系的教学主要由一个大纲规定每一门课所需讲授的内容，而大纲中对所授内容的顺序以及课本的选择等都是没有要求的。我们希望保证授课老师能有充分大的自由度来设计他所讲授的内容和进度。这样的自由度能有助于各个老师充分发挥自己所长，也能由此让同学们感受到更多的东西。事实上，这是大学教学不同于中学教学的一个主要方面，可以

说，大学的教材都是参考书，不像中学那般模式化的教学。这种教授的自主性将在一定程度上帮助同学们在学习上产生主动性吧。

笔者：的确，大学的学习更多在课外。之前我们有说到科大的应数专业，在这里我是指广义上的应用数学，包括计算数学这个方向，由于科大重视基础的大背景，感觉它在很大程度上与纯数专业相似，应用性似乎不够。虽然学校里有一些如数学建模竞赛之类的与应用数学有关的活动，但是好像数学系同学的积极性不太大。请问陈老师对此有什么看法呢？

陈老师：我觉得，我们的应用数学专业主要是培养两类人才。第一类是立志于从事各方面研究的人才，比如生物数学、金融数学领域。对这些想今后做研究的应数方向的同学，数学和物理是他们最重要的基础。我相信“挑战杯”，电磁学论文竞赛能给他们提供一个很好的交流和应用的平台。第二类是希望投身于具体的实际研究的人才。对他们来说，最重要的是把所学的东西给用出去。而建模竞赛是检验和展示他们这种能力的舞台。其实，对数学系，尤其是学应用数学这个方向的同学来说，GPA绝对不是唯一检验大家的标准，多参加一些这样的活动，尤其是建模竞赛，提高自身的综合素质，让自己的亮点多起来，对大家今后的帮助会更大。而这些应用型的活动，可以作为大家今后从事实际研究的一个很好的过渡。另外，学校里还有“大学生研究计划”，去香港科大、台湾清华以及UCLA的交流项目，同学们多参加一些这样的活动，走出书本，通过和别的学校甚至国家的人交流，开阔自身视野，也许比简单地提高0.01的GPA更好。对了，还想强调一下，对于学习所设置的应用数学这个小方向的同学来说，物理以及计算数学的很多课程其实是很重要的，希望大家能在自己的专业选修课里有所考虑。

笔者：陈老师的教导对我们很受用。但是我个人觉得，应数方向的同学更多拘泥于书本，也和科大“重视基础”的宣传分不开的。我想这个宣传在一定程度上对同学们有所误导，让大家以为基础重于一切吧。我想，是否可以请系里，或者是一些任课老师对同学们多做一些有关这些活动的介绍和宣传呢，让大家对它们有更深的认识。另外，您之前提到了一些交流项目，但是就我们05级同学的观察，好像这些交流的机会并不多，想请问今后数学系是否会考虑增加这类活动呢？

陈老师：刚刚的建议很好，我们今后会做相关的努力。当然，由于系里的老师大多从事纯数的研究，往往在授课时只讲授理论，而对于理论的来源与最终的应用介绍很少。这样不太利于学生牢固掌握和灵活应用所学知识，也会让教学过程显得枯燥，我们在今后会注意改进。对于交流项目，这将是未来的一个趋势，数学系目前在和学校商讨，考虑拿出一部分资金来增加与香港大学的一些交流项目。另外，我们也在考虑增加一些和大陆其他高校的短期交流项目，就像05级与华师大数学系的交流那样。至于和国外大学的交流，由于这需要校方之间签订相关协议，会麻烦一些，不过相信今后这样的交流也会增加。

笔者：非常感谢陈老师的介绍。刚刚我们讨论的主要与应数有关，下面我们说说纯数的话题。之前我们有讨论到，应用数学方向可能增加专业选修课的数目，那么对于纯数专业，是否会有类似的考虑呢？我记得曾经有师兄抱怨，说数学系代数类的课程不够。

陈老师：是这样的，在整个中国的数学系都存在这样的现象：分析类的课程很多，代数类的较少，几何类的更少。这和现今中国从事代数及几何方面研究的人才较少有很大关系。其实科大在代数和几何方面设置的课程比国内绝大多数高校数学系设置得多和难。当然，随着“华罗庚班”的设立，我们在这个方面将有更多的改进。由于“华罗庚班”的学生后两年将在中科院进行教学，那边各个方向的人才都很多，将会考虑在代数、几何方向增加课程数量和难度，如代数拓扑、流形的课程，争取满足对这些方向感兴趣的同学吧。当然也可以考虑增设分析类的课程。

笔者：那样真的很好。不过，我们通过对之前数学系的“出口”观察，感觉科大数学系毕业的学生很少有人会继续从事数学方向的研究，特别是纯数学。想请问陈老师觉得这样的现象是否正常呢？

陈老师：这个问题很好。我认为，科大数学系的出口应该分成两个大类，一类是继续从事基础数学研究，一类就是从事广义上的应用数学方向的工作。我们希望数学系学生的出口是多元化的，有一小部分人追随自己的兴趣，对相关理论进行研究，而更多的同学是将自己所学的数学给用出去。即使大家今后的工作看起来和数学似乎没有相关性，但是你们的思维方式、方法，会因为学过数学而更加缜密，富有逻辑性。而这些，我想是非数学系的同学，从一定程度上来说，所缺乏的吧。

笔者：的确，我们不能指望所有数学系的同学今后都去做纯数的研究，数学的学习更多给与我们的是思维的锻炼。但是，是否有这样的可能性呢：很多同学目前仅仅接触到很少的数学分支，他们往往仅通过自己对这些有限分支的“没感觉”来断定自己对整个纯数学研究没有兴趣。我们想，系里能不能开一些讲座什么的，对数学的各个分支，或者一些目前的前沿研究做一些简单的介绍呢？这样，也许会有更多的同学考虑将来做理论研究呢。

陈老师：你建议的这些其实我们目前正在筹备。我们设想举办一系列的科普性的讲座和报告，主要邀请国内一些数学大家，以及科大在国外的校友来做主讲人，介绍一些有趣的数学分支以及一些前沿性的研究。当然，如果有机会，我们也会邀请一些世界上的数学大家来做报告。例如下个月，张伟平院士将到系里来做一个科普讲座。今后这样的讲座和报告将会越来越多，希望同学们能够多来参加。

笔者：非常期待下个月的报告会。说到数学研究，这里还有一个有关大学生研究计划的问题想请教陈老师。请问大研的时间是规定在大三暑期的么？同学们平时是否能参与一些研究项目呢？

陈老师：大研的时间没有硬性规定，只是大多数同学选择在那个时间参与这个项目。实际上，只要同学们觉得自己已经准备好了，可以随时考虑联系系里甚至外系（在假期里还可以联系中科院）的老师进行自己的大研项目。书籍购买或其他经费什么的可以向系里提出申请。等数学系搬到新楼去后，我们将考虑选出一间教室专门用作同学们研究讨论的场所。我

在数学里，分辨何事重要，何事不重要，知所选择是很重要的。

—— 广中平佑

觉得，本科生的研究重在过程，感受一种经历和了解真实研究，最终结果并不重要。另外，其实每学期都会有老师向系里申报自己的研究项目，同学们可以到时来系里了解一下，如果有自己感兴趣而且有所准备的方向，可以和有关老师联系参与这些项目的研究。对于这些消息，我们将考虑今后放在系里主页的合适位置，方便同学们查阅。

笔者：那样同学们将有更多的机会亲身参与到自己感兴趣的研究项目中了，感谢系里的这些工作。除了之前我们聊到的话题外，也有很多同学想了解一下科大数学系的团队建设。下面的这个问题可能有些敏感。想请问一下陈老师，您对科大数学系一些老师的流失有什么看法呢？现在数学系从理学院中独立了出来，成为学校的直属系后，这个现象是否会有所改善呢？

陈老师：首先我给大家介绍一下导致这个现象的几个原因吧。一来是数学这个学科本身的特点。对于物理化学等涉及到实验室和相关仪器的学科，由于研究对仪器和实验室的依赖，人员流动会比较少。而数学由于不存在这些考虑，所以本身的流动性会大一些。二来，我们也应该看到地域的差异性对这个现象的影响。另外，之前学校的一些政策也可能导致此。现在，随着我们系成为学校的直属系，很多政策能有所改进，而且近年来交通、交流局限性慢慢减少，网络方面比以前有很大进步，地域差异对此流失现象的影响力正慢慢减弱。另外，我们在考虑通过为年轻老师提供上升空间、广阔交流平台以及宽松的氛围等方式，为数学系的老师创造更好的环境。科大本身来说要留住一个人才比清华、北大要困难许多，但我们科大本身就有一种不服输的韧劲，如果我们创造了一个很好的环境并且持续做下去，相信我们将在留住人才和引进人才上面做得更好！

笔者：我们对数学系的明天有信心！说到引进人才，这里有同学建议：很多大学聘请一些国际上知名的数学家担任名誉教授，比如丘成桐先生就是清华等大学的名誉教授，我们科大数学系是否可以考虑做类似的举动呢？

陈老师：数学系可以考虑聘请一些名誉教授。但是，由于名誉教授一般一年中能给同学们见面的机会没几次，所以名誉教授更多的仅是对学校或系里名声的增加，同学们从中受益并不大。我想，如果请一些科大在国外的成功校友或者一些相较不那么出名的数学家来科大做各类报告，或者做一段时间的访问学者，教授一些短期的课程，能够给年轻老师和同学们更多的熏陶吧。我们更倾向于做一些实质性的事情。现在国家还有一个“千人计划”，即全职聘请一些国外知名大学的正教授在国内学校任教。我们系已经联系了Wisconsin的陈秀雄教授。不过，由于国外的校友一般只有暑期比较方便，所以之前提到的那些模式的报告和课程很可能只能安排在假期。我们在考虑通过如暑期学校之类的方式解决这个问题。

笔者：我们期待着今后数学系师与生的共同人才济济。不知不觉时间过去了好多，很感谢陈老师和我们聊了这么久，我们从这次谈话中了解了很多，也学到了很多。最后，想请问陈老师有什么话想对数学系的同学们说的么？

陈老师：首先，还是想强调一下，希望同学们不要“唯GPA是论”，GPA绝对不是大家大学生活的唯一内容。平时多参加一些活动，除了之前所说的建模赛等应用型的活动外，也可

多参加一些社团活动，以及听一些人文方面的讲座，培养自己各方面的能力和素养。另外，希望大家不要闭塞自己，多互相交流，主动去寻求和争取机会锻炼及展示自己，希望大家的大学生活过得充实而快乐！

笔者：我代表数学系的全体学生再次感谢您接受我们这次采访！

封面相关介绍

卡拉比-丘流形

数学上，卡拉比　丘流形（Calabi　Yau manifold）是一个的第一陈类为0的紧致n维凯勒流形，也叫做卡拉比　丘n-流形。数学家卡拉比在1957年猜想所有这种流形（对于每个凯勒类）有一个里奇平坦流形的度量，该猜想于1977年被丘成桐证明，成为丘定理（Yau's theorem）。因此，卡拉比　丘流形也可定义为“紧里奇平坦卡拉比流形”(compact Ricci-flat Kähler manifold)。

也可以定义卡拉比　丘n流形为有一个SU(n)和乐（holonomy）的流形。再一个等价的定义是流形有一个全局非0的全纯(n,0)-形式。

卡拉比猜想

卡拉比猜想源于代数几何，是由意大利著名几何学家卡拉比在1954年国际数学家大会上提出的:在封闭的空间，有无可能存在没有物质分布的引力场？卡拉比认为是存在的，可是没有人能证实，包括卡拉比自己。

美籍华裔数学家丘成桐27岁攻克几何学上难题“卡拉比猜想”，并因此在1982年(33岁)获得数学界的“诺贝尔奖”　　菲尔兹奖，是迄今为止惟一获得该奖的华人数学家。

丘成桐简介

1976年，丘成桐解决微分几何中的“卡拉比猜想”，声誉鹊起。这猜想源出于代数几何，为意大利E.卡拉比于1954年所提出。这是给定里奇曲率求黎曼度量的问题，其中需要求解一个很难的偏微分方程，丘成桐解决了这个难题。他的成功,促使一大批同类方程得到解决,成果累累，取得了代数几何学、复解析几何学、微分几何学甚至广义相对论等领域的一系列重要定理。1978、1979年丘成桐与R.舍恩应用微分几何方法，造极小曲面，运用非线性方程的技巧，证明了广义相对论中的正质量猜想。此外，在高维闵科夫斯基问题、塞梵利猜想（与肖荫堂合作）、弗兰克尔猜想、三维流形的拓扑学与极小曲面和史密斯猜想等方面均有成就。1981年获美国数学会颁发的维布伦奖，1982年又获费尔兹奖(1983年8月16日在华沙颁发)。以后还获各种奖多次。

早晨醒来，想的第一件事就是数学。我的生活就是数学；终生不倦地追求就是数学，数十年如一日，从没有懈怠过，现在依然如此。

—— 陈省身

蛙鸣编委的毕业去向

张韵华

1981年6月20日，为了创建学生之间共同探讨、自由交流数学的园地，由科大数学系78级本科生自发组织，自写、自编、自刻、自印的油印刊物第一期"蛙鸣"刊物，这是80年代国内数学系学生自编的第一本刊物，第一期的《蛙鸣》编委有王翎（航天部720所博士，国创公司创始人和首席执行官）、胡森（美国普林斯顿大学博士，中国科技大学教授，中科院"百人计划"入选者）、鄂维南（美国普林斯顿大学教授，曾获美国总统奖、应用数学学会科拉兹奖）、莫小康（美国斯坦福大学博士，被华尔街日报誉为中国的Bloomberg）、汪洋（哈佛大学博士，密西根州立大学数学系主任）、施皖雄（哈佛大学博士，师从丘成桐教授）。

从1981年到2008年历经27届毕业生共完成62期，近300名学生担任了《蛙鸣》编委。《蛙鸣》也得到数学系各届领导和教授的支持和关注。张景中、单　、李尚志、王树禾、程艺、张贤科和余红兵等教授都曾给《蛙鸣》提供过不少问题和修订稿件。

参加《蛙鸣》投稿的学生都是对数学有兴趣数学基础好的优秀学生，在写稿、录入和排版的过程中，培养了学生分析和解决问题的能力，也给学生提供了探索数学的空间，如今已在国际顶尖数学杂志Ann. Math.发表多篇论文的沈维孝（91级本科生）的第一篇论文发表94年第49期《蛙鸣》中，论文的题目是"一个有关矩阵极小秩的问题"。沈维孝教授是中科院"百人计划"入选者，2009年4月荣获第十二届中国数学会"陈省身数学奖"。

几乎所有的《蛙鸣》编委本科毕业后都选择继续深造，在国内外的读研比例高达99%以上，如今已有很多《蛙鸣》的学生编委已成长为国内外数学界的科研和教学的帅才，以及金融、信息等企业的领军人物。《蛙鸣》已成为展示科大数学系本科生风采的靓丽风景！

下表是57期至63期蛙鸣编委毕业去向：

入学年级	姓名	性别	期刊号	就业去向（全部读研）
2000	蔡云峰	男	57	北京大学（保研）
2000	李元	男	57	中国科学技术大学（保研）
2000	卢献	男	57	中科院数学与系统科学研究院
2000	罗栗	男	57	中科院数学与系统科学研究院
2000	魏靖	男	57	中国科技大学（考研）
2001	沈明民	男	58	美国哥伦比亚大学
2001	李勤	男	58	美国加州大学伯克利分校
2001	黄宇发	男	58	香港科技大学（保研）
2001	马宇超	男	58	中科院数学与系统科学研究院

入学年级	姓名	性别	期刊号	就业去向（全部读研）
2001	刘杭	男	58	中科院数学与系统科学研究院
2001	杨勤荣	男	58	上海科学院（考研）
2001	罗振斌	男	58	美国约翰霍普金斯大学
2002	修大成	男	59, 60	美国普林斯顿
2002	雷涛	男	59, 60	加拿大约克
2002	张智	男	59, 60	美国莱斯大学
2002	王可	女	59, 60	美国罗特格斯大学
2002	金天灵	男	59, 60	美国罗特格斯大学
2002	张鹏飞	男	59, 60	中科大（保研）、中美联合培养
2002	孙俊	男	59, 60	中科院数学与系统科学研究院
2002	王麒翰	男	59, 60	中国科学技术大学（保研）
2002	张翔雄	男	59, 60	美国布朗大学
2002	胡雪莹	女	59, 60	美国密西根大学
2002	刘欣	女	59, 60	美国北卡大学
2003	申述	男	61	法国巴黎高工
2003	常智华	男	61	中国科学技术大学（保研）
2003	刘博	男	61	南开大学（保研）
2003	袁媛	女	61	纽约大学库朗研究院
2003	张振	男	61	香港科技大学（保研）
2003	姚远	女	61	香港科技大学（保研）
2003	黄丽全	女	61	美国特拉华大学
2004	管枫	男	62	加州大学洛杉矶分校
2004	洪继展	男	62	加拿大麦克马斯特
2004	薛航	男	62	美国哥伦比亚大学
2004	张伟哲	男	62	美国佐治亚理工学院
2004	李果	男	62	浙江大学保研
2004	罗世森	男	62	美国康奈尔大学
2004	孙祥	男	62	新加波国立大学
2004	王岚晖	女	62	美国普林斯顿大学
2004	叶晗	女	62	美国北卡罗纳大学
2005	涂思铭	男	63	中科大（保研）
2005	杨扬	男	63	美国布朗大学
2005	王晓辉	男	63	美国俄亥俄州立
2005	华淼	男	63	中科院数学与系统科学研究院
2005	汪颖佩	男	63	美国莱斯大学
2005	杨馨	女	63	美国莱斯大学
2005	杨熠	女	63	美国加州大学洛杉矶分校

A mathematician is a device for turning coffee into theorems.

—— Paul Erdos

预处理共轭梯度法解位势方程

05001 陈争

摘 要

由普通物理的背景，我们知道位势方程是个很典型的方程问题，对于它的求解方法的研究具有很强的实际意义。下面举一个例子说明:

分布在三维空间区域Ω上的静电场的电位函数u(x, y, z)，若Ω内的电荷密度为ρ(x,y,z),则u满足Poisson 方程$-\Delta u = 4\pi\rho(x,y,z)$.

这就是我们要处理的对象，经过差分方法或者有限元方法研究在三维区域$\Omega = [0,1]\times[0,1]\times[0,1]$离散方程后得到一个大型的方程组Ax=b，其中A 是大型稀疏矩阵，针对这个方程的迭代数值解法，我们在下面将会具体介绍并举例比较优缺点。

§1 算法介绍

⋆ 不完全因子分解法

对于大型矩阵通过高斯消去进行LU 分解是个耗时耗力的工作，这里要讲的不完因子分解法是针对稀疏矩阵，预先制定一个指标集J，算法仅对(i,j)∈J 执行，以大为降低运算量。通常选择的J 是对称的，下面给出伪代码:

$Input\ n, (a_{ij})$
$For\ k = 1\ to\ n\ do \quad a_{kk}^k = sqrt(a_{kk}^{k-1})$
$If(j > k\ \&\ (k,j) \in J)\ then\ a_{kj}^k = a_{kj}^{k-1}/a_{kk}^k$
$If(i > k\ \&\ (i,k) \in J)\ then\ a_{ik}^k = a_{ik}^{k-1}/a_{kk}^k$
$If(i > k\ \&\ j > k\ \&\ (i,k) \in J\ \&\ (k,j) \in J\ \&\ (i,j) \in J)\ then\ a_{ij}^k = a_{ij}^{k-1} - a_{ik}^k a_{kj}^k$
End

为了使这个算法稳定，需要在运行过程中$|a_{kk}^k|$不至于太小，因此出现改进不完全因子分解法，下面给出一种比较常用的方法。

⋆ 修改不完全因子分解法

此法的宗旨是使逐步演化的主元不致过小。设K是N 阶方阵,J 是二元指标集，由A^r到A^{r+1}演断由以下算法实现:

$$\hat{A}_{kk}^k = \left\{ \begin{array}{c} A_{kk}^k, if\ S_k^{(r)} \geq \alpha A_{kk}^k \\ A_{kk}^k + \delta_k, if\ S_k^{(r)} \leq \alpha A_{kk}^k \end{array} \right\}$$

$$l_{ik} = A_{kk}^k / \hat{A}_{kk}^k$$

$$A_{ij}^{k+1}=\left\{\begin{array}{c} A_{ij}^{k}-l_{ik}A_{kj}^{k},\ if\ (k+1\le j\le N)\bigcap[(i,j)\in J]\bigcap(i\neq j) \\ 0,\ if\ (k+1\le j\le N)\bigcap[(i,j)\notin J] \\ A_{ii}^{k}-l_{ik}A_{ki}^{k}\sum_{p=k+1\ and\ (i,p)\notin J}^{N}(A_{ip}^{k}-l_{ik}A_{kp}^{k}),\ if\ i=j \end{array}\right\}$$

其中，$k=1,2,...,N-1;i=r+1,...,N;\alpha\in(0,1)$是选定的值，且

$S_r^{(r)}=\sum_{j=k}^{N}A_{kj}^{k}$

$\delta_k=\frac{\alpha^2}{1-\alpha}A_{kk}^{k}+\frac{\alpha}{1-\alpha}max(t_k^{(1)}-t_k^{(0)},0)$

$t_k^{(0)}=\sum_{i=1}^{k-1}(-A_{ik}^{i}),t_k^{(1)}=\sum_{j=r+1}^{N}(-A_{kj}^{k})$

经过细致分析表明此法等价于对矩阵$\hat{A}$做未修改不完全因子分解算法，其中$\hat{A}=A+diag(\sigma_i\delta_1,...,\sigma_{(N-1)}\delta_{(N-1)},0)$,

$$\delta_k=\left\{\begin{array}{c} 1,if\ S_k^{(r)}\ge\alpha A_{kk}^{k} \\ 0,if\ S_k^{(r)}\le\alpha A_{kk}^{k} \end{array}\right\}$$

此法通过r=1,...,N-1逐步推断，定义了N 阶阵$\hat{A}^{k+1}$,其元素为

$$\hat{A}_{ij}^{(k+1)}=\left\{\begin{array}{c} A_{ii}^{k},i=1,...,k \\ A_{ij}^{k},i=1,...,k,j=i+1,...N \\ A_{ij}^{k+1},i,j=k+1,...,N \\ 0,others \end{array}\right\}$$

,其中$\hat{A}^1=K$

如此即可得到非奇异的上三角阵$\hat{U}=\hat{A}^N$和一个下三角阵L,其元素为

$$\hat{I}_{ij}=\left\{\begin{array}{c} l_{ij},i>r \\ 1,i=r \\ 0,i<r \end{array}\right\}$$

• 预处理共轭梯度法

当系数矩阵的特征值比较均匀的分布在一个很长的区间上时，共轭梯度法的收敛速度可能会变得很慢。这种情况在实际应用中却经常遇到。因此，如何提高其迭代速度非常重要。如果能够选取一个非奇异矩阵C，是$\tilde{A}=C^{-1}AC^{-T}$的特征值分布在一个较小的区间内，或分布较为“集中”的话，那么应用共轭梯度法于新的方程组$\tilde{A}\tilde{x}=\tilde{b}$中，$\tilde{x}=C^Tx,\tilde{b}=C^{-1}b$,将会有较快的收敛速度，进而可以提高求解元方程组的速度。记$M=CC^T$,叫做预优矩阵。算法如下:

1) 输入A, M, b 和b_0

$r_0:=b-Ax_0$; $z_0:=M^{(-1)}r_0$; $p_1:=z_0$;$\rho_0:=r_0^TZ_0$ $k:=1$

2)$\omega=Ap_k,\alpha_k:=p_{k-1}/p_k^T\omega$

$x_k=x_{k-1}+\alpha p_k,r_k:=r_{k-1}-\alpha_k\omega$; $z_k:=M^{-1}r_k,\rho_k=r_k^Tz_k$

$\beta_k:=\rho_k/\rho_{k-1},p_{k+1}:=z_k+\beta_kp_k$

3) 如果$\rho_k<\rho_0\varepsilon$,则输出x_k,; 否则k:= k+1，转步2)

预优矩阵M 应该具有如下特征:

每当我的头脑没有问题思考时，我就喜欢将已经知道的定理重新验证一番。这样做并没有什么目的，只是让自己有个机会充分享受一下专心思考的愉快。
—— 爱因斯坦

a) M 对称正定;

b) M 应该与A 的稀疏性差不多;

c)$M^{-1}A$(即$\tilde{A}=C^{-1}Ac^{-T}$)的特征值分布“集中”;

d) 形如Mz = r 的方程组容易求解,即M 应具有某些特殊性形状,如块对角,或三角矩阵的乘积(例如,ILUPCG,MILUPCG)。

例:

⋆ SSOR-PCG

SSOR 中迭代公式可等价表示为:

$x^{k+1}=Bx^k+M^{-1}b$

其中

$B=(\frac{1}{\omega}D+L^*)^{-1}[(\frac{1}{\omega}-1)D-L](\frac{1}{\omega}D+L)^{-1}[(\frac{1}{\omega}-1)D-L^*]$

$M=\frac{1}{2-\omega}(\frac{1}{\omega}D+L)(\frac{1}{\omega}D)^{(-1)}(\frac{1}{\omega}D+L)^*$

用这里的M 作为PCG 算法的预优矩阵,即得到SSOR-PCG。

优点:

a) 最优SSOR-PCG 的收敛速度,比CG 法的收敛速度快一个数量级,尤其是A 的条件≫1时更有效;

b) 它的收敛速度对ω 的选取并不敏感。

⋆ ILU-PCG

在不完全因子分解法中,A 被分解为A=C+R,其中$C=LL^T$,LLT,R 为剩余,可证明C 是正定的,R 是非负的,由于计算$C^{-1}g$是容易的,所以不完全因子分解预处理共轭梯度法可以表示如下:

$x=x^0;g=b;\ g=Ax-g;h=C^{-1}g;d=-h;\delta_0=(g,h)$

$if(\delta_0<\varepsilon)\ then\ stop$

R: h=Ad

$\tau=\delta_0/(d,h);x=x+\tau d;\ g=g+\tau h$

$h=C^{-1}g;\delta_1=(g,h)$

$if\ (\delta_1\le\varepsilon)\ then\ stop$

$\beta=\delta_1/\delta_0;\delta_0=\delta_1;\ d=-h+\beta d$

goto R

⋆ MILU-PCG

MILU-PCG 就是用$\hat{C}=\hat{L}\hat{U}$(其中$\hat{L}$和$\hat{U}$是前面修改不完全因子法中提到的$\hat{L}$和$\hat{U}$))作为预处理矩阵解方程Ax=b。如果A 对称正定,就可以分解$\hat{C}=\hat{L}\hat{D}\hat{L}^T$,其中$\hat{D}=diag(\hat{A}^1_{11},...,\hat{A}^N_{NN}$是对角阵。

在有些情况下,MILU-PCG 比CG 可能要快一个数量级。

§2 举例分析

在这里我们以对偏微分方程初值问题

$$\left\{\begin{array}{c}-\Delta u=f\ in\ \Omega=[0,1]\times[0,1]\times[0,1]\\ u=u^0,on\ \partial\Omega\end{array}\right\}$$

求解为例进行研究对比已经熟知的SSOR,CG 和三种预处理共轭梯度法SSOR-PCG,ILU-PCG, MILU-PCG:

对于偏微分方程的求解方法SSOR,CG,SSOR-PCG,ILU-PCG, MILU-PCG 进行编程，对于精确解u 为以下4 种时，进行结果比较，其中网格分割数$n_x = n_y = n_z = 64$，error 是数值解U 与精确解在各结点取值相差的最大值，即绝对误差。

1)

$$\left\{ \begin{array}{c} -\Delta u = 0 \ in \ \Omega = [0,1] \times [0,1] \times [0,1] \\ u = 1, on \ \partial\Omega \end{array} \right\}$$

有精确解u=1

64	time	error	times
ssor	253.297	1.18E-08	584
cg	60.031	4.09E-10	179
ssor-pcg	23.922	3.09E-10	12
ilu-pcg	35.5	5.73E-10	79
milu-cg	1.203	3.61E-14	1

2)

$$\left\{ \begin{array}{c} -\Delta u = 0 \ in \ \Omega = [0,1] \times [0,1] \times [0,1] \\ u = x, on \ \partial\Omega \end{array} \right\}$$

有精确解u=x

64	time	error	times
ssor	257.485	7.44E-09	577
cg	89.359	3.06E-10	245
ssor-pcg	27.578	8.24E-11	14
ilu-pcg	41.625	3.99E-10	93
milu-cg	21.609	5.94E-11	48

3)

$$\left\{ \begin{array}{c} -\Delta u = -4 - 12z^2 \ in \ \Omega = [0,1] \times [0,1] \times [0,1] \\ u = x^2 + y^2 + z^4, on \ \partial\Omega \end{array} \right\}$$

有精确解$u = x^2 + y^2 + z^4$

64	time	error	times
ssor	257.656	2.74E-05	567
cg	90.078	2.74E-05	245
ssor-pcg	27.547	2.74E-05	14
ilu-pcg	41.359	2.74E-05	93
milu-cg	23.359	2.74E-05	52

4)

$$\left\{ \begin{array}{c} -\Delta u = -sinh(x) \ in \ \Omega = [0,1] \times [0,1] \times [0,1] \\ u = sinh(x), on \ \partial\Omega \end{array} \right\}$$

有精确解$u = sinh(x)$

64	time	error	times
ssor	269.719	6.70E-07	575
cg	88.047	6.70E-07	245
ssor-pcg	27.641	6.70E-07	14
ilu-pcg	41.437	6.70E-07	93
milu-cg	22.531	6.70E-07	50

从这些数据可以明显看出:

1. 在运算量上, CG 比SSOR 少得多;

2.而相比较而言, SSOR-PCG,ILU-PCG, MILU-PCG 的运算量更加小;

3. MILU-PCG较ILU-PCG 具有明显优势.

§3 总结评论

从较短的时间和极小的误差, 我们可以看出, 以上各种迭代法在求解某些偏微分方程数值解(例如: 对称正定)中, 的确可以得到比较接近的近似解。所以在对解的精确性的要求有限的时候, 可以尝试采取迭代法求解偏微分方程。

对称逐次超松弛法(SSOR)和共轭梯度法(CG)已经能够满足求解较精确近似解的要求, 但是SSOR-PCG, ILU-PCG, MILU-PCG 能够大量减少工作量, 在较短的时间内得到精确性很高的近似解, 因而更具有优越性。

对于无法求得精确解得位势方程边值问题, 在这里没有进行实际检验结果误差, 但是可以猜测预处理共轭梯度法在求解这些问题时也会体现良好的性质。

参考文献

[1] Numerical Analysis–Mathematics of Scientific Computing,(Third Edition). by David Kincaid & Ward Cheney,China Machine Press

[2] 偏微分方程,(第二版)陈祖墀编著, 中国科学技术大学出版社

[3] 区域分解算法–偏微分方程数值解新技术, 吕涛, 石济民, 林振宝著, 科学出版社

[4] 矩阵计算的理论与方法, 徐树方编著, 北京大学出版社

三道ACM题目的数学理论

05001 杨扬

摘 要

本文以三题为例，简要说明数学在ACM中的威力。程序要求在2000毫秒内通过全部测试点，至多占用2M内存

§1 问题一

在$n \times n$的棋盘上放$2n$个皇后，要求每行、每列有且只有2个皇后。我们认为两种摆放方式是相同的，如果经过行互换和列互换之后变成一样的，问不同的摆放方式有多少种？

显然在1×1的棋盘上没有满足条件的摆放方式;在2×2的棋盘上只有一种。为了方便，我们在棋盘上引入坐标，从左上角方格起第a行，第b列方格坐标为(a,b)。由于可以对棋盘上的皇后做行互换和列互换。这样总可以将皇后换到$(1,1),(1,2)$和$(2,2)$的位置上。

定义1.1. 在$n \times n$的格阵上,皇后位于$(1,n),(i,j)$,其中$j+1 \geq i \geq j$,所形成的摆放方式叫做一个n块。

由此可知在2×2的棋盘上唯一的摆放方式就是2块。下面考虑$n \geq 3$的情况，利用数学归纳法的思想，将棋盘逐步扩大。假设在$n \times n$的棋盘上摆放方式为将n块中$(1,n)$处的皇后去掉所形成，棋盘扩大，继续摆放皇后。第n列有两个位置，$(1,n)$和$(n+1,n)$。(事实上，行坐标可以大于$n+1$，此时可以将皇后经过行互换换到$(n+1,n)$ 处)对于前者，得到一个n块，这样在前n行和n列中就不会再有其他皇后了，我们可以在余下的棋盘上重新开始工作; 对于后者，考虑列坐标大于n的列，总可以经过列互换将皇后放在$(n+1,n+1)$，这就回到了前面的讨论。至此，我们得到每一个摆放方式都是由m块组成的图案$(m=2,\cdots,n)$。显然不同的块互换位置后得到同样的摆放方式。至此我们得到

命题1.1. 两个摆放方式不同当且仅当组成这个摆放方式的m块的个数不全相同$(m=2,\cdots,n)$

在上述命题的基础上,我们给出原问题的解答

命题1.2. 不同的摆放方式的个数等于不定方程$2x_2+\cdots+(n-2)x_{n-2}=n$的非负整数解的个数加1

证明. 先假设摆放方式可以分成至少两个块。事实上，设m块的个数为x_m，每个m块占据了棋盘上的m行。显然，对于$n \times n$的棋盘，$n-1$块和1块是不存在的，这样棋盘上的总行数就是$2x_2+\cdots+(n-2)x_{n-2}$。由命题1.2，上述方程中的每个非负整数解与每种摆放方式一一对应。此外只剩下一个n块的摆放方式。 □

利用组合数学的生成函数很容易的到问题的解。题目非常简单，我们不给出程序代码。

§2 问题二

给出三个正整数a,b,c，以及一种操作：将其中一个数(例如a)乘以2，再用另一个数(例如b)减去a，保证操作后三个数仍为正整数，现要求将原来的三个数经过若干次上述操作变成相同的数，问是否可以完成。如果可以，给出每次操作结束后的结果。其中a,b,c均为不超过50的正整数。

我们下面的命题都是建立在可以完成的假设下。令$y=a+b+c$，显然有

命题2.1. $3 \mid y$

令$x=\frac{y}{3}, d=(a,b,c)$，则有

命题2.2. $d \mid x$

证明. 每一步操作相当于对矩阵(a,b,c)做两次初等列变换，即右乘形如$\begin{pmatrix} 2 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$的矩阵。容易看出，这样的矩阵一共有6个，且其元素均为整数，于是存在整系数矩阵A使得$(a,b,c)A=(x,x,x)$，所以$d \mid x$ □

注 命题2.2表明只需要考虑$d=1$即可

定义2.1. 上述6个形如$\begin{pmatrix} 2 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$的矩阵叫做操作矩阵

令$x=2^k t$，t为奇数，

命题2.3. $t \mid d$

证明. 操作矩阵(不妨取$\begin{pmatrix} 2 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$)的逆为$\begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$，这样矩阵$A$(定义同命题2.2)的逆中的元素的分母均为2的方幂，由于$(a,b,c)=(x,x,x)A^{-1}$，则$(a,b,c)=t(\frac{x}{t},\frac{x}{t},\frac{x}{t})A^{-1}$，因为$t$为奇数，所以$(\frac{x}{t},\frac{x}{t},\frac{x}{t})A^{-1}$为整系数矩阵，故$t \mid d$ □

注 命题2.3告诉我们只需要考虑$x=2^k$即可

下面的命题是本题算法的基础

命题2.4. 如果$d=1$，且$a \le b \le c$，则a,b中至少有一个是奇数，进一步如果a,b中只有一个奇数，则c为奇数

证明. 假设a,b均为偶数，则$2 \le a \le b$，因为$d=1$，所以c为奇数，故x为奇数，由命题2.3知$x \mid d$，故$x=1$，于是$a+b+c=3$，这与$a+b+c \ge 4$矛盾。进一步，如果a,b中只有一个奇数且c为偶数，则x为奇数，同理得到矛盾 □

定义2.2. 设$(a\ b\ c)$为某次操作结束后的结果,称这三个数的最大公约数d为放大因子;如果$d=1$,则称$(a\ b\ c)$为基本数对

下面给出算法，不妨设$a\le b\le c, d=1$
如果$a=b=c$则问题有解，结束程序，否则继续。
如果a,b均为奇数，则将(a,b,c)变为$(2a,b,c-a)$，放大因子不变;
如果a为奇数，b为偶数，则将(a,b,c)变为$(a,\frac{b}{2},\frac{c-a}{2})$，放大因子乘以2;
如果b为奇数，a为偶数，则将(a,b,c)变为$(\frac{a}{2},b,\frac{c-b}{2})$，放大因子乘以2
重复上述步骤直至将基本数对变成$(1,1,1)$为止

命题2.5. 上述算法是正确的

证明. 首先，每一步操作结束后所得到的数对均为基本数对。容易看出，至多2次操作，放大因子就增加一倍，故至多经过$2k$次，放大因子等于2^k，此时$a+b+c=3$，故$a=b=c=1$。 □

命题2.6. 问题有解的充要条件是$t\mid d$且$d\mid x$

证明. 必要性已证，下面证明充分性。由已知设$d=2^l k(l\le k)$，初始置放大因子为d，基本数对为$(\frac{a}{d},\frac{b}{d},\frac{c}{d})$，根据算法可以得到问题的解。 □

注 $d\mid x$不可去，例如$(3,9,12)$无解，此时$t=1,d=3,x=8$;$t\mid d$不可去，例如$(1,2,6)$无解，此时$t=3,d=1,x=3$

§3 问题三

记F_N为一个数组，它由集合$G_N=\{\frac{a}{b}\mid (a,b)=1,a<b\le N\}$中的元素从小到大排列。给定一个正整数$k$，问$F_N$中的第$k$个数是多少，其中$k<N<10^9$

我们考虑连分数展开，因为有这种表示方法的分数一定是既约分数。作为尝试，我们只展开一步，将每个分数写成$\frac{1}{a+\frac{c}{b}}$的形式，其中$c<b$。
显然有

命题3.1. 设$t_i=\frac{x_i}{y_i}=\frac{1}{a_i+\frac{c_i}{b_i}}$为$F_N$中的元素，则$(x_i\ y_i)=1\Leftrightarrow(b_i\ c_i)=1$

命题3.2. 如果$a_i<a_j$或者$a_i=a_j$且$\frac{c_i}{b_i}<\frac{c_j}{b_j}$，则$t_i>t_j$

任务似乎已经完成了，只需按照不同的a_i将F_N分组，确定第k个数在哪一组，就可以递归下去，直至问题解决。但如何判断第k个数在哪一组很困难

命题3.3. a的取值可以小于$\frac{N}{k}$的充分必要条件是b可以取k

证明. 充分性，因为b可以取k，则$ak+c\le N$，所以$ak<N$，即a可以小于$\frac{N}{k}$;必要性，因为$a<\frac{N}{k}$，所以$ak<N$，故$ak+1\le N$，即b可以取k □

推论3.1. 当$a\ge\frac{N}{4}$时，b不可能取4

One can imagine that the ultimate mathematician is one who can see analogies between analogies.

—— Stefan Banach

命题3.3描述了a与b的取值关系，但c的取值并不容易得出。事实上，令$T=[\frac{N}{a}]$，取$b\le T$，即使$c\le b$，$\frac{c}{b}$却不一定属于F_T。例如$N=100$，$\frac{1}{33+\frac{1}{3}}$在F_N中而$\frac{1}{33+\frac{2}{3}}$就不在；另外，计算F_T的元素个数也很困难。但是,对于b很小时,我们总可以解决上述问题

推论3.2. 当b可以取3时，$\frac{c}{b}$的值只有$\frac{2}{3}$可能取不到

我们还有一个条件$K<N$没有用到

命题3.4. $b\le 3$

证明. 由推论3.1我们期望在$a\ge\frac{N}{4}$时，a,b,c的不同取值产生满足要求的分数个数$S\ge N-1$。
当$a\ge\frac{N}{2}$时,a至少有$N-(\frac{N}{2}+\frac{1}{2})=1=\frac{N+1}{2}$种取值，
当$\frac{N}{2}>a\ge\frac{N}{3}$时,$a$至少有$\frac{N}{2}-1-(\frac{N}{3}+\frac{2}{3})+1=\frac{N-4}{6}$种取值，
当$\frac{N}{3}>a\ge\frac{N}{4}$时$a$至少有$\frac{N}{3}-1-(\frac{N}{4}+\frac{3}{4})+1=\frac{N-9}{12}$种取值。
所以当$N\ge 18$时$S\ge\frac{N+1}{2}+2\times\frac{N-4}{6}+4\times\frac{N-9}{12}-1\ge N-\frac{11}{6}$，由于$S$为整数，故$S\ge N-1$；
当$10\le N\le 17$且$\frac{N}{3}>a\ge\frac{N}{4}$时，$a$至少有1种取值，所以$S\ge\frac{N+1}{2}+2\times\frac{N-4}{6}+3\ge N-1$;
当$N=9$且$\frac{N}{2}>a\ge\frac{N}{3}$时$a$有2种取值，所以$S\ge\frac{N+1}{2}+4=N$;
当$5\le N\le 8$且$\frac{N}{2}>a\ge\frac{N}{3}$时$a$至少有1种取值，所以$S\ge\frac{N+1}{2}+2\ge N-\frac{3}{2}$，由于$S$为整数，故$S\ge N-1$。
当$N\le 4$时，显然b的取值至多是3 □

注 上面所用的分数($\frac{N+1}{2}$, $\frac{N-4}{6}$和$\frac{N-9}{12}$)等可能不是整数，我们理解为下界。

下面给出算法

若$K\le N-[\frac{N-1}{2}]$，则第K个数为$1/(N-K+1)$;
若$K-(N-[\frac{N-1}{2}])\le 2[\frac{N+1}{2}]-2[\frac{N+2}{3}]$，令$L=K-N-[\frac{N-1}{2}]$
若L为偶数，则第K个数为$1/([\frac{N+1}{2}]-\frac{L}{2})$;
否则，则第K个数为$2/(2[\frac{N+1}{2}]-L)$;
其他情况，令$L=K-(N-[\frac{N-1}{2}])-2([\frac{N+1}{2}]-[\frac{N+2}{3}])$,
当$K\equiv 1(mod3)$时，
若$L\equiv 0(mod4)$则第K个数为$3/(3[\frac{N+2}{3}]-3[\frac{L}{4}]-1)$;
若$L\equiv 1(mod4)$则第K个数为$2/(2[\frac{N+2}{3}]-2[\frac{L}{4}]-1)$;
若$L\equiv 2(mod4)$则第K个数为$3/(3[\frac{N+2}{3}]-3[\frac{L}{4}]-2)$;
若$L\equiv 3(mod4)$则第K个数为$1/([\frac{N+2}{3}]-\frac{L+1}{4})$;
当$K\equiv 0,2(mod3)$时，若$L\equiv 0(mod4)$则第K个数为$1/([\frac{N+2}{3}]-\frac{L}{4})$;
若$L\equiv 1(mod4)$则第K个数为$3/(3[\frac{N+2}{3}]-3[\frac{L}{4}]-1)$;
若$L\equiv 2(mod4)$则第K个数为$2/(2[\frac{N+2}{3}]-2[\frac{L}{4}]-1)$;
若$L\equiv 3(mod4)$则第K个数为$3/(3[\frac{N+2}{3}]-3[\frac{L}{4}]-2)$.

第二题和第三题程序如下:

第二题程序

```
main()
{
  int a,b,c,d=1,i,x,m,j,k,t,l=0;
  int p[15]={2,3,5,7,11,13,17,19,23,29,31,37,41,43,47},q[3];
  scanf("%d%d%d",&a,&b,&c);
  if ((a+b+c)%3!=0) printf("error\n");
    else t=x=(a+b+c)/3;
  for (i=0;i<15;)
    if (a%p[i]==0&&b%p[i]==0&&c%p[i]==0) d*=p[i],a/=p[i],b/=p[i],c/=p[i];
    else i++;
  while(t%2==0)
  {
    t/=2;
    l++;
  }
  if (d%t||x%d) printf("error\n"),exit(0);
  printf("%d %d %d\n",a*d,b*d,c*d);
  for (m=1;m<=2*l;m++)
  {
    if (a<b)
      if (b<c) p[0]=0,p[1]=1,p[2]=2;
      else
    if (a<c) p[0]=0,p[1]=2,p[2]=1;
    else p[0]=1,p[1]=2,p[2]=0;
    else
      if (c<b) p[0]=2,p[1]=1,p[2]=0;
      else
    if (a<c) p[0]=1,p[1]=0,p[2]=2;
    else p[0]=2,p[1]=0,p[2]=1;
    i=j=k=0;
    q[0]=a,q[1]=b,q[2]=c;
    while (p[i]!=0) i++;
    while (p[j]!=1) j++;
    while (p[k]!=2) k++;
    if (q[i]%2)
      if (q[j]%2) q[k]-=q[i],q[i]*=2;
      else d*=2,q[j]/=2,q[k]=(q[k]-q[i])/2;
    else q[i]/=2,q[k]=(q[k]-q[j])/2,d*=2;
    a=q[0],b=q[1],c=q[2];
    printf("%d %d %d\n",a*d,b*d,c*d);
    if (a==b&&b==c) break;
  }
}
```


I have had my results for a long time: but I do not yet know how I am to arrive at them.

—— Carl Friedrich Gauss

第三题程序

```
main()
{
  int n=29,k,l;
  while(k!=0)
  {
  scanf("%d",&k);
  if (k<=n-(n-1)/2) printf("1/%d\n",n-k+1);
    else if (k-n+(n-1)/2<=(n+1)/2*2-(n+2)/3*2)
        {
          l=k-n+(n-1)/2;
          switch(l%2)
          {
            case 1:printf("2/%d\n",(n+1)/2*2-l);break;
            case 0:printf("1/%d\n",(n+1)/2-l/2);break;
          }
        }
        else
            {
          l=k-(n-(n-1)/2)-((n+1)/2*2-(n+2)/3*2);
          switch (n%3)
          {
            case 1:switch(l%4)
                {
                  case 0:printf("3/%d\n",(n+2)/3*3-1-l/4*3);break;
                  case 1:printf("2/%d\n",(n+2)/3*2-1-l/4*2);break;
                  case 2:printf("3/%d\n",(n+2)/3*3-l/4*3-2);break;
                  case 3:printf("1/%d\n",(n+2)/3-(l+1)/4);break;
                };break;
            case 0:
            case 2:switch(l%4)
                {
                  case 0:printf("1/%d\n",(n+2)/3-l/4);break;
                  case 1:printf("3/%d\n",(n+2)/3*3-1-l/4*3);break;
                  case 2:printf("2/%d\n",(n+2)/3*2-1-l/4*2);break;
                  case 3:printf("3/%d\n",(n+2)/3*3-2-l/4*3);break;
                }
          }
        }
  }
}
```

由一道线性代数题目想到

05001　杨扬

本文从一道线线性代数题目出发，分析发现题目错误，给出结论成立的充分必要条件，给出了三种证明。

曾经在一本线性代数书上见到这样一个题目

设$A \in R^{m\times n}, B\in R^{n\times m}$,证明: $rank(AB) = rank(BA)$的充分必要条件是存在$C \in R^{m\times n}$，使得$A = ABC$,并由此证明如果$AB = ABAB$，则$BA = BABA$.

对题目的分析

第一问比较简单，利用解空间就可以解决，这里不做过多叙述

对于第二问直观上有两种处理方式:

1. 将A, B视为孤立的矩阵，利用相抵标准型，这样计算量会很大
2. 将AB与BA视为两个整体，但是从AB转化到BA很困难.

作为探路石，我们先考虑第一种方法。

方法一

令

$$A = P_A \begin{pmatrix} I_{r_A} & 0 \\ 0 & 0 \end{pmatrix} Q_A,$$

$$B = P_B \begin{pmatrix} I_{r_B} & 0 \\ 0 & 0 \end{pmatrix} Q_B,$$

带入原式得到

$$\begin{pmatrix} I_{r_A} & 0 \\ 0 & 0 \end{pmatrix} Q_A P_B \begin{pmatrix} I_{r_B} & 0 \\ 0 & 0 \end{pmatrix} Q_B P_A \begin{pmatrix} I_{r_A} & 0 \\ 0 & 0 \end{pmatrix} Q_A P_B \begin{pmatrix} I_{r_B} & 0 \\ 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} I_{r_A} & 0 \\ 0 & 0 \end{pmatrix} Q_A P_B \begin{pmatrix} I_{r_B} & 0 \\ 0 & 0 \end{pmatrix}$$

假设我们要证明的结论成立，由于该结论等价于

$$\begin{pmatrix} I_{r_B} & 0 \\ 0 & 0 \end{pmatrix} Q_B P_A \begin{pmatrix} I_{r_A} & 0 \\ 0 & 0 \end{pmatrix} Q_A P_B \begin{pmatrix} I_{r_B} & 0 \\ 0 & 0 \end{pmatrix} Q_B P_A \begin{pmatrix} I_{r_A} & 0 \\ 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} I_{r_B} & 0 \\ 0 & 0 \end{pmatrix} Q_B P_A \begin{pmatrix} I_{r_A} & 0 \\ 0 & 0 \end{pmatrix}$$

在令

$$\begin{pmatrix} I_{r_A} & 0 \\ 0 & 0 \end{pmatrix} Q_A P_B \begin{pmatrix} I_{r_B} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} X & 0 \\ 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} I_{r_B} & 0 \\ 0 & 0 \end{pmatrix} Q_B P_A \begin{pmatrix} I_{r_A} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} Y & 0 \\ 0 & 0 \end{pmatrix},$$

之后，上面两式可化简为

$$XYX = X, \tag{0.1}$$

$$YXY = Y, \tag{0.2}$$

然而从(0.1)不一定能推出(0.2)

反例如下

$$X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, Y = X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

请读者自行验证

寻找结论成立的充要条件

很明显，由秩不等式可知

$$rang(AB) = rank(ABAB) \leq rank(BA)$$

另一方面，在结论成立的假设下有

$$rank(BA) = rank(BABA) \leq rank(AB)$$

所以，如果结论成立，条件

$$rank(AB) = rank(BA)$$

是必不可少的。

然而这是否是充要条件呢？我们回到(0.1)与(0.2),并假设

$$rank(X) = rank(Y)$$

设

$$X = P_X \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} Q_X, Y = P_Y \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} Q_Y$$

其中$r = rank(X) = rank(Y)$带入(0.1)和(0.2)得到

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} Q_X P_Y \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} Q_Y P_X \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

If indeed, as Hilbert asserted, mathematics is a meaningless game played with meaningless marks on paper, the only mathematical experience to which we can refer is the making of marks on paper.

—— E. T. Bell

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} Q_Y P_X \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} Q_X P_Y \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

上述两式显然是等价的

至此，我们得到了此题的充要条件是

$$rank(AB) = rank(BA)$$

方法二

下面我们将AB与BA视为整体，必须将AB转化到BA，这就是加入新条件所起的作用

从参考文献[1]中我们直接借用一个基本结论:

设n阶方阵满足条件$A^2 = A$,则存在可逆方阵P使得

$$P^{-1}AP = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

其中$r = rank(A)$

实际上不难证明这是个充要条件

这样我们可以选取可逆矩阵P使得

$$P^{-1}ABP = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \tag{0.3}$$

结论转化为证明存在可逆矩阵Q，使得

$$Q^{-1}ABQ = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \tag{0.4}$$

我们声明过，在这种做法中将AB, BA视为整体，在(0.3)的等式两边分别乘以B，但是需要先将P^{-1}放到等式右边，得到

$$BABP = BP \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \tag{0.5}$$

我们继续将BP视为整体，把BA解出来

先将BP尽量简单的分块，只需要按列分块就可以了，因此令

$$BP = (X\ Y)$$

带入(0.5)得到

$$BAX = X \tag{0.6}$$

显然$rank(X) \leq r$，只需要证明$rank(X) \geq r$就可以利用基扩充定理将BA从(0.6)中解出

由(0.6)得

$$rank(X) \geq rank(AX),$$

As far as extra dimensions are concerned, very tiny extra dimensions wouldn't be perceived in everyday life; just as atoms aren't: we see many atoms together but we don't see atoms individually.

—— Edward Witten

由(0.3)得

$$ABP = P\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix},$$

因此AX就是$P\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$的前$r$列，所以

$$rank(AX) = r,$$

故

$$rank(X) \geq r$$

利用基扩充定理将X扩充成为可逆矩阵$(X\ Z)$，得到

$$BA(X\ Z) = (X\ BAZ)$$

由新加入的已知条件得

$$rank(BA(X\ Z)) = r,$$

所以$(Z\ BAZ)$中X就自然成为该矩阵的一个极大无关组，所以存在初等矩阵

$$R = \begin{pmatrix} I_r & M \\ 0 & I_{n-r} \end{pmatrix}$$

使得

$$(X\ 0)R = (X\ BAZ),$$

从而推出

$$XM = BAZ, \tag{0.7}$$

因此我们得到

$$BA = (X\ 0)\begin{pmatrix} I_r & M \\ 0 & I_{n-r} \end{pmatrix}(X\ Z)^{-1},$$

我们大胆的猜想

$$(X\ Z) = Q,$$

只需要证明

$$(X0)\begin{pmatrix} I_r & M \\ 0 & I_{n-r} \end{pmatrix} = Q\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

利用(0.7)有

$$(X\ 0)\begin{pmatrix} I_r & M \\ 0 & I_{n-r} \end{pmatrix} = (X\ Z)\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} I_r & M \\ 0 & I_{n-r} \end{pmatrix} = (X\ Z)\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} = Q\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

至此，我们给出了第二个证明

方法三

我们利用利用线性变换的思想

设V和W分别是m维和n维的线性空间，A为$W \to V$的线性变换，B为$V \to W$的线性变换。

故AB为$V \to V$的线性变换，BA为$W \to W$的线性变换

我们借用参考文献[1]的结论:

矩阵可以相似对角化的充分必要条件是该矩阵存在一组线性无关的特征向量。

由于$AB = ABAB$,故AB的极小多项式整除多项式$x^2 - x$，故AB的特征值只有0和1。

由于BA与AB有相同的特征值(事实上，任取λ 为AB的特征值，设$ABx = \lambda x$，则有$BABx = b\lambda x = \lambda Bx$，所以$\lambda$也为$BA$的特征值)所以$BA$的特征值也只有0和1。

从方法二种我们知道AB可以相似对角化，故有一组线性无关的特征向量不妨记为

$$\alpha_1, \alpha_2, \cdots, \alpha_n,$$

其中前r个为特征值1对应的特征向量，其他为特征值0对应的特征向量.

对于$1 \leq j \leq r$，有

$$AB\alpha_j = \alpha_j,$$

所以

$$BABB\alpha_j = B\alpha_j.$$

这说明$B\alpha_j$为BA的特征值1的特征向量，容易证明$B\alpha_1, B\alpha_2, \cdots, B\alpha_r$线性无关。

由已知条件

$$rank(AB) = rank(BA)$$

知

$$Im(AB) = Im(BA),$$

所以$\{B\alpha_j\}, 1 \leq j \leq r$就构成了$Im(BA)$的一组基，取$ker(AB)$的一组基$\beta_1, \beta_2, \cdots, \beta_{n-r}$，这样

$$B\alpha_1, B\alpha_2, \cdots, B\alpha_r, \beta_1, \beta_2, \cdots, \beta_{n-r}$$

就构成了BA的一组线性无关的特征向量

回到最初的题目，我们发现以上三种方法都没有用到第一问的结论，有兴趣的读者可以尝试利用该结论证明此题。

参考文献

[1] 线性代数，李尚志，2006.5

If a dog jumps in your lap, it is because he is fond of you; but if a cat does the same thing, it is because your lap is warmer.

—— Alfred North Whitehead

关于 r 为无理数 $\{nr\}$ 的估计

05001 谢俊逸

我们知道 $\{nr\}$ 在 $[0,1]$ 区间是等分布的，所以有时 $\{nr\}$ 会突然变得很小，所以对 $\{nr\}$ 的下界做估计是有意义的，不过我不能在一般的情况下给出具体的估计，但是当 r 为代数无理数时，估计可以做得很好。

定理1. 若 r 为代数无理数，r 的最小多项式次数为 d，则对 $\forall \varepsilon > 0$，$\exists C > 0$，使得 $\{nr\} \geqslant \frac{C}{n^{d-1+\varepsilon}}$。

证明. 设 $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ 是 r 的最小多项式，其中 $a_i \in Z, a_d \neq 0, i = 0,1,2,\cdots d$。
假设结论不成立，则对 $\forall N > 0$，$\exists n_1$，使得 $\{n_1 r\} < \frac{1}{Nn^{d-1+\varepsilon}}$，
即 $\exists m_1$，使得 $| n_1 r - m_1 | < \frac{1}{Nn_1^{d-1+\varepsilon}}$，也就是 $| r - \frac{m_1}{n_1} | < \frac{1}{Nn_1^{d+\varepsilon}}$，对 $\forall k \in N$，$\exists m_k, n_k$，使得 $| r - \frac{m_k}{n_k} | < \frac{1}{kNn_k^{d+\varepsilon}} < \frac{1}{Nn_k^{d+\varepsilon}}$。
由于 $| r - \frac{m_k}{n_k} | \neq 0$ 以及 $\frac{1}{kN} \to 0$，从而有无穷多的 $\frac{m_k}{n_k}$ 使得 $| r - \frac{m_k}{n_k} | < \frac{1}{Nn_k^{d+\varepsilon}}$。
注意到 $| r - \frac{m_k}{n_k} | < 1$，令 $\max\limits_{|x-r|\leqslant 1} | f'(x) | = M$。
因为 $f(r) = 0$，则有 $| f(\frac{m_k}{n_k}) | = | f(r) - f(\frac{m_k}{n_k}) | \leqslant M | r - \frac{m_k}{n_k} | < \frac{M}{Nn_k^{d+\varepsilon}}$，从而有 $| n_k^d f(\frac{m_k}{n_k}) | < \frac{M}{Nn_k^{\varepsilon}}$。
令 $k \to \infty$，则 $n_k \to \infty$，这是因为对于固定的 ε 和 n，使 $| r - \frac{m}{n} | < \varepsilon$ 的 m 有限。
所以有 $| n_k^d f(\frac{m_k}{n_k}) | \to 0 (k \to \infty)$，即有无穷多的 $\frac{m_k}{n_k}$ 使得 $| n_k^d f(\frac{m_k}{n_k}) | < 1$.
注意到 $| n_k^d f(\frac{m_k}{n_k}) | = | a_k m_k^d + \cdots + a_0 n_k^d |$ 是整数，所以当 k 充分大时，$| n_k^d f(\frac{m_k}{n_k}) | = 0$，这说明 $f(x) = 0$ 有无穷多个根，矛盾。
所以 $\exists N_0 > 0$，使得 $\{nr\} \geqslant \frac{1}{N_0 n^{d-1+\varepsilon}}$，取 $C = \frac{1}{N_0}$ 即可。 □

定理2. 关于一般情况:

*1.*对 $\forall a_m > 0$，如果 $\sum\limits_{m=1}^{\infty} a_m < +\infty$，则使得有无穷多 m，$\exists n$，有 $| mr - n | < a_m$ 的 r 为零测集。

*2.*对 $\forall a_m > 0$，如果 $\sum\limits_{m=1}^{\infty} a_m < +\infty$，$\exists$ 无理数 r，有无穷多的 m，使 $\exists n$，有 $| mr - n | < a_m$。

*3.*将 *1,2* 中的 $| mr - n | < a_m$ 改为 $\{nr\}$ 结论仍成立。

证明. *1.*m 充分大时，即 $\exists N_0$，$m \geqslant N_0$，有 $\frac{a_m}{m} < 1$，此时若 r 满足 $| mr - n | < a_m$，即 $| r - \frac{n}{m} | < \frac{a_m}{m}$，所以有 $| \{r\} + [r] - \frac{n}{m} | < \frac{a_m}{m}$，因此 $| [r] - \frac{n}{m} | - \{r\} < \frac{a_m}{m}$，所以 $| [r] - \frac{n}{m} | < \frac{a_m}{n} + 1 < 2$，因此有 $m[r] - 2m \leqslant n \leqslant m[r] + 2m$。

令 E 为题中要求的集合，则 $E = \bigcup\limits_{k \in Z} E_k$，其中

$$\begin{aligned} E_k &= \bigcap_{M=1}^{\infty}\bigcup_{m\geqslant M}^{\infty}\bigcup_{n=1}^{\infty}(\tfrac{n}{m}-\tfrac{a_m}{m},\tfrac{n}{m}+\tfrac{a_m}{m})\bigcap[k,k+1) \\ &= \bigcap_{M=M_1}^{\infty}\bigcup_{m\geqslant M}^{\infty}\bigcup_{n=1}^{\infty}\{(\tfrac{n}{m}-\tfrac{a_m}{m},\tfrac{n}{m}+\tfrac{a_m}{m})\bigcap[k,k+1)\} \\ &\subset \bigcap_{M=1}^{\infty}\bigcup_{m\geqslant M}^{\infty}\bigcup_{mk-2m\leqslant n\leqslant mk+2m}(\tfrac{n}{m}-\tfrac{a_m}{m},\tfrac{n}{m}+\tfrac{a_m}{m}) \end{aligned}$$

这是因为 $r\in E_k$，$r\in[k,k+1)$，所以 $[r]=k$。

所以有

$$\begin{aligned} \mu(E_k) &\leqslant \mu(\bigcap_{M=M_1}^{\infty}\bigcup_{m\geqslant M}^{\infty}\bigcup_{mk-2m\leqslant n\leqslant mk+2m}(\tfrac{n}{m}-\tfrac{a_m}{m},\tfrac{n}{m}+\tfrac{a_m}{m})) \\ &\leqslant m(\bigcap_{m\geqslant M}^{\infty}\bigcup_{mk-2m\leqslant n\leqslant mk+2m}(\tfrac{n}{m}-\tfrac{a_m}{m},\tfrac{n}{m}+\tfrac{a_m}{m}))(\forall M\geqslant M_1) \\ &\leqslant \sum_{m\geqslant M}^{\infty}(2m+1)\times 2\tfrac{a_m}{m} \\ &\leqslant \sum_{m\geqslant M}^{\infty}5m\times 2\tfrac{a_m}{m} \\ &= 10\sum_{m\geqslant M}^{\infty}a_m \end{aligned}$$

令 $M\to\infty$，则可得 $\mu(E_k)=0$，所以有 $\mu(E)=\mu(\bigcup_{k\in Z}E_k)=0$，从而结论成立。

2.因为 $E=\bigcap_{M=1}^{\infty}(\bigcup_{m\geqslant M}^{\infty}\bigcup_{n=1}^{\infty}(\tfrac{n}{m}-\tfrac{a_m}{m},\tfrac{n}{m}+\tfrac{a_m}{m}))$，所以 E 为 G_δ 集，又 $Q\subset E$，但是 Q 不是 G_δ 集，所以 $\exists r\in E\setminus Q$，故结论 2 成立。

3.与 1 对应的性质，因为 $\{mr\}<a_m$，所以 $\exists n$，使得 $|mr-n|<a_m$，所以性质 1 成立。

与 2 对应的性质，我们所求的集合是 $E=\bigcap_{M=1}^{\infty}(\bigcup_{m\geqslant M}^{\infty}\bigcup_{n=1}^{\infty}(\tfrac{n}{m}-\tfrac{a_m}{m},\tfrac{n}{m}+\tfrac{a_m}{m}))$，则 E 为稠密开集之交，所以 E 在 R 上稠，E 为 G_δ 集，E 不可数，$E\not\subset Q$，所以 $\exists r\in E\setminus Q$，$r$ 即为所求。 □

我们从证明中发现，研究 $\inf\limits_{n\in Z}|mr-n|$ 比 $\{mr\}$ 更自然，而对 $\inf\limits_{n\in Z}|mr-n|$，上述结果可以照搬。

对 $\inf\limits_{n\in Z}|mr-n|$ 还有一个估计，可以作为我们原来估计的反面。

定理3. 对任意无理数 r，有 $\inf\limits_{k\leqslant n}\inf\limits_{m\in Z}|kr-m|<\frac{1}{n}$。

证明. $\{r\},\{2r\}\cdots\{nr\}\subset(0,1)$，若 $\forall\{kr\}\notin(0,\frac{1}{n})$，$1\leqslant k\leqslant n$。则有 $\{\{kr\}\}_{k=1,2\cdots n}\subset(\frac{1}{n},\frac{2}{n})\bigcup(\frac{2}{n},\frac{3}{n})\cdots(\frac{n-1}{n},1)$，则 $\exists k\in\{1,2\cdots n-1\}$，$i,j\in\{1,2\cdots n\}$，$i<j$，使得 $\{ir\},\{jr\}\in(\frac{k}{n},\frac{k+1}{n})$，所以有 $|\{ir\}-\{jr\}|<\frac{1}{n}$，即为 $|(j-i)r+([ir]-[jr])|<\frac{1}{n}$，从而 $\inf\limits_{m\in Z}|(j-i)r-m|<\frac{1}{n}$，因此有 $\inf\limits_{k\leqslant n}\inf\limits_{m\in Z}|kr-m|<\frac{1}{n}$。 □

特别的，对于 $r=\sqrt{2}$，有 $\inf\limits_{k\leqslant n}\inf\limits_{m\in Z}|k\sqrt{2}-m|<\frac{1}{n}$，又根据定理 1，有 $\inf\limits_{k\leqslant n}\inf\limits_{m\in Z}|k\sqrt{2}-m|\geqslant\frac{C}{n^{1+\varepsilon}}$，从而有 $\frac{C}{n^{1+\varepsilon}}\leqslant|n\sqrt{2}-m|<\frac{1}{n}$。

由康托尔的工作所带来的哲学革命也许甚至比数学本身还要伟大。

—— 约代因

$GL_n(Q)$, $GL_n(Z)$ 的一些有趣性质

05001 谢俊逸

定理1. $GL_n(Q)$ 在 n 不同时互不同构，$GL_n(Z)$ 也是。

证明. 事实上对任意特征不是2 的整环 D，$GL_n(D)$ 在 n 不同时互不同构。
$GL_n(D)$ 有子群 $H=\{\mathrm{diag}(a_1,a_2\cdots a_n)\mid a_i=\pm 1,i=1,2\cdots n\}$，同构于 Z_2^n。
又如果有子群 A 同构于 Z_2^n，则 $A\subset GL_n(D)\subset GL_n(K)\subset GL_n(\overline{K})$，
其中 K为 D 的商域，$\overline{K}$ 为 K 的代数闭包，
则 A 在 $GL_n(\overline{K})$ 中可同时对角化，即存在 $g\in GL_n(\overline{K})$，使得 $g^{-1}Ag=A'\in\{diag(a_1,a_2,\cdots,a_n)\mid a_i\in\overline{K},i=1,\cdots,n\}$，则有 A' 同构于 Z_2^m。
所以对 $\forall h\in A'$，有 $h^2=I$，$h\in H$，所以有 $A'\subset H$，从而有 $\mid Z_2^m\mid\leqslant 2^n$，即 $2^m\leqslant 2^n$，
故有 $m\leqslant n$，即 n 为最大的使 $GL_n(D)$ 含有同构于 Z_2^m 的子群的 m，从而命题得证。 □

定理2. 对 $\forall n$，$\exists M(n)$，使得任意 $GL_n(Q)$ 的任意有限子群的阶不大于 $M(n)$。

证明. $\forall g\in GL_n(Q)$，若 $\exists m$，使得 $g^m=I$，令 d_g 为 g 的最小多项式，则有 $d_g(x)\mid x^m-1$，
所以 $d_g(x)=\prod_{\text{某些}d\mid m}\Phi_d(x)$，这是因为 x^m-1 无重根，从而 $d_g(x)$ 无重根，所以 $\Phi_d(x)$ 两两不同，令这些 d 的集合为 S。
因为 $deg(d_g(x))\leqslant n$，所以有 $deg(\Phi_d(x))\leqslant n$，又因为 $deg(\Phi_d(x))=\Phi(d)$，所以有 $\Phi(d)\leqslant n$。
设 $d=p_1^{r_1}\cdots p_t^{r_t}$，其中 $p_1<p_2<\cdots<p_t$，则 $\Phi(d)=p_1^{r_1-1}(p_1-1)\cdots p_t^{r_t-1}(p_t-1)$，
因为 $p_1\geqslant 2$，所以有 $p_i\neq 2(2\leqslant i\leqslant t)$，则 $p_i-1\geqslant 2$，从而有 $n\geqslant\Phi(d)\geqslant(p_2-1)\cdots(p_t-1)\geqslant 2^{t-1}$，所以有 $t\leqslant\log_2 n+1$。
对任意 $1\leqslant i\leqslant t$，$p_i-1\leqslant n$，所以 $p_i\leqslant n+1$，$2^{r_i-1}\leqslant p_i^{r_i-1}\leqslant n$，从而有 $r_i\leqslant\log_2 n+1$，
所以有 $d=p_1^{r_1}\cdots p_t^{r_t}\leqslant[(n+1)^{\log_2 n+1}]^{\log_2 n+1}=(n+1)^{(\log_2 n+1)^2}$，所以 $S\subset\{1,2\cdots[(n+1)^{(\log_2 n+1)^2}]+1\}$。
故 $d_g(x)=d_g(x)=\prod_{d\in S}\Phi_d(x)\quad\prod_{d\mid([(n+1)^{(\log_2 n+1)^2}]+1)!}\Phi_d(x)=x^{([(n+1)^{(\log_2 n+1)^2}]+1)!}-1$。
令 $N(n)=([(n+1)^{(\log_2 n+1)^2}]+1)!$，则 $g^{N(n)}=I$，则对 $GL_n(Q)$ 的任意有限子群 G，对任意 $g\in G$，有 $g^{|G|}=I$。
由前面的论证知，$g^{N(n)}=I$，从而 g得特征值为 $x^{N(n)}-1=0$ 的根，
令 $tr(g)\in\{\sum_{i=1}^{n}\alpha_i\mid\alpha_i^{N(n)}-1=0\}=T$，设 G 在 $GL_n(Q)$中张成的线性空间 $<G>$ 维数为 l，
则有 $l\leqslant n^2$。
令 $g_1,g_2\cdots g_l$ 为 $<G>$ 的一组基，令 $\Psi:G\to T^l$，有 $\Psi(g)=(tr(gg_1),tr(gg_2)\cdots tr(gg_l))$。
若有 $\Psi(g)=Psi(h)$，设 $g^{-1}=\sum_{i=1}^{l}x_ig_i$，所以有 $n=tr(gg^{-1})=\sum_{i=1}^{l}x_itr(gg_i)=\sum_{i=1}^{l}x_itr(hg_i)=tr(h\sum_{i=1}^{l}x_ig_i)=tr(hg^{-1})$。
因为 hg^{-1}得特征值为 $x^{N(n)}-1=0$ 的根，所以 $tr(hg^{-1}=n$ 说明 hg^{-1} 的特征值全为 1，

因为 $d_{hg^{-1}}(x) \mid x^{N(n)}-1$ 无重根，所以 hg^{-1} 可对角化，又其特征值全为 1，所以有 $hg^{-1}=I$，即 $h=g$，故 Ψ 为单射，所以 $\mid G \mid \leqslant \mid T \mid^l \leqslant \mid T \mid^{n^2} \leqslant (N(n)^n)^{n^2} = N(n)^{n^3}$，令 $M(n) = N(n)^{n^3}$，则命题得证。 □

因为 $GL_n(Z) < GL_n(Q)$，所以上述结论对 $GL_n(Z)$也成立，但是可以用另外的方法得出更精确的估计。

对任意 $GL_n(Z)$的子群 G，$p \neq 2$ 为素数，令 $\varphi : GL_n(Z) \to GL_n(F_p)$ 为模 p 约化，即

$$\varphi\left(\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}\right) = \begin{vmatrix} \overline{a_{11}} & \overline{a_{12}} & \cdots & \overline{a_{1n}} \\ \overline{a_{21}} & \overline{a_{22}} & \cdots & \overline{a_{2n}} \\ \cdots & \cdots & \cdots & \cdots \\ \overline{a_{n1}} & \overline{a_{n2}} & \cdots & \overline{a_{nn}} \end{vmatrix}$$

其中 $\overline{x}$ 是 x 模 p 的等价类。

对任意 $g \in G$，有 $g^{|G|} = I$，令 $\mid G \mid = p^\alpha m$，其中 $(m,p)=1$，则若 $\varphi(g) = I$，如果 $g \neq I$，则 $g = I + p^i A$，$A \in M_n(Z)$，$\overline{A} \neq 0$，则 $g^p = I + p^{i+1}A + C_p^2 p^{2i} A^{2i} + \cdots + C_p^p (p^i A)^p$。

因为 $p \mid C_p^2, \cdots C_p^{p-1}$，$ip > p+1$，所以有 $g^p = I + p^{i+1}A + p^{i+2}B$，其中 $B \in M_n(Z)$，所以有 $g^p = I + p^{i+1}A_1$，$A_1 \in M_n(Z)$，$\overline{A_1} \neq 0$。

类似可得 $g^{p^2} = I + p^{i+2}A_2$，$A_2 \in M_n(Z)$，$\overline{A_2} \neq 0$，$\cdots\cdots$，$g^{p^\alpha} = I + p^{i+\alpha}A_\alpha$，$A_\alpha \in M_n(Z)$，$\overline{A_\alpha} \neq 0$，$I = (g^{p^\alpha})^m = (I + p^{i+\alpha}A_\alpha)^m = I + mp^{i+\alpha}A_\alpha + \cdots + (p^{i+\alpha}A_\alpha)^m$，

由于 $\overline{mA_\alpha} \neq 0$，所以有 $I = I + p^{i+\alpha}D$，其中 $\overline{D} \neq 0$，矛盾。

所以一定有 $g = I$，即 φ 为单射，从而有 $\mid G \mid \leqslant \mid GL_n(F_p) \mid$，取 $p=3$，则有 $\mid G \mid \leqslant \mid GL_n(F_3) \mid = (3^n-1)(3^n-3)\cdots(3^n-3^{n-1})$。

If I have seen farther than others, it is because I was standing on the shoulders of giants.

—— Isaac Newton

高维线性波动方程初值问题求解公式

05001 汪颖佩

摘 要

本文主要讨论在一定条件下，以下问题的求解公式（其中c是给定的常数）：

$$\begin{cases} u_{tt} - c^2\Delta u = f(x,t) & \forall x \in \mathbb{R}^n, t \in \mathbb{R} \\ u = \varphi(x) & \forall x \in \mathbb{R}^n, t = 0 \\ u_t = \psi(x) & \forall x \in \mathbb{R}^n, t = 0 \end{cases} \tag{0.1}$$

§1 前言

在陈祖墀老师编著的偏微分方程课本中，分别给出了低维齐次波动方程的*d'Alembert*公式，*Kirchhoff* 公式和*Poision*公式.但无论哪一个公式的表达式都是相当复杂的，使用起来很不方便.本文在添加一定条件后，直接给出了任意维的波动方程的解的一个较为简单的表达式，然后用*Duhamel*原理将问题推广到非其次的情形.接着讨论了本文中问题的唯一性和稳定性.最后用几个例子比较了本文的求解公式和课本中公式求解结果的一致性和难以区别.

§2 两个引理

引理2.1. 若$\psi(x) \in \mathbb{C}^4(\mathbb{R}^n)$满足$\Delta^2\psi = 0$,则下述问题:

$$\begin{cases} u_{tt} - c^2\Delta u = 0 & \forall x \in \mathbb{R}^n, t \in \mathbb{R} \\ u = 0 & \forall x \in \mathbb{R}^n, t = 0 \\ u_t = \psi(x) & \forall x \in \mathbb{R}^n, t = 0 \end{cases} \tag{2.1}$$

有$\mathbb{C}^2$解: $u(x,t) = \psi(x)t + \frac{1}{6}c^2\Delta\psi(x)t^3$.

证明. 这是引理2.2的一个特例，在此略去证明。 □

引理2.2. 若$\varphi(x), \psi(x) \in \mathbb{C}^4(\mathbb{R}^n)$满足$\Delta^2\varphi = 0, \Delta^2\psi = 0$,则下述问题:

$$\begin{cases} u_{tt} - c^2\Delta u = 0 & \forall x \in \mathbb{R}^n, t \in \mathbb{R} \\ u = \varphi(x) & \forall x \in \mathbb{R}^n, t = 0 \\ u_t = \psi(x) & \forall x \in \mathbb{R}^n, t = 0 \end{cases} \tag{2.2}$$

有$\mathbb{C}^2$解: $u(x,t) = \varphi(x) + \psi(x)t + \frac{1}{2}c^2\Delta\varphi(x)t^2 + \frac{1}{6}c^2\Delta\psi(x)t^3$.

证明. 令$u(x,t)=\varphi(x)+\psi(x)t+\frac{1}{2}c^2A(x)t^2+\frac{1}{6}c^2B(x)t^3$,
以上假设的$u(x,t)$已经满足了初值条件，将其再代入方程有:
$[A(x)+tB(x)]-c^2[\Delta\varphi(x)+\Delta\psi(x)t+\frac{1}{2}\Delta A(x)t^2+\frac{1}{6}\Delta B(x)t^3]=0$,
上式对任意的$t\geq 0$成立，从而有:
$A(x)=c^2\Delta\varphi(x), B(x)=c^2\Delta\psi(x), \Delta A(x)=0, \Delta B(x)=0$,
其中后两式与已知条件刚好相符.
从而本问题的一个$\mathbb{C}^2$解为:
$u(x,t)=\psi(x)t+\frac{1}{6}c^2\Delta\psi(x)t^3$. □

注：证明中对$u(x,t)$那么假设的原因是将$u(x,t)$看作t的函数，并在t处作$Taylor$展开，那些t的更高阶的导数项由于本问题的条件特殊性并未在解的表达式中出现.这是因为如果假设$u(x,t)$是光滑的,这些高阶(4阶以上)的项在条件下都是0.这么处理的问题一方面在于并不知道$u(x,t)$是不是光滑的，我们并不能对它直接作$Taylor$展开.另一方面它只是给出了问题的一个$\mathbb{C}^2$解,保证了解的存在性,并给出了解的表达式. 在本文最后将证明本问题解的唯一性,并在有限时间内讨论解的稳定性.

§3 主要结果

定理4. 若$\varphi(x),\psi(x)\in\mathbb{C}^4(\mathbb{R}^n), f(x,t)\in\mathbb{C}^4(\mathbb{R}^n\times[0,\infty))$,且满足: $\Delta^2\varphi=0,\Delta^2\psi=0,\Delta_x^2f(x,t)=0$,则下述$Cauchy$问题:

$$\begin{cases} u_{tt}-c^2\Delta u=f(x,t) & \forall x\in\mathbb{R}^n, t\in\mathbb{R} \\ u=\varphi(x) & \forall x\in\mathbb{R}^n, t=0 \\ u_t=\psi(x) & \forall x\in\mathbb{R}^n, t=0 \end{cases} \tag{3.1}$$

有$\mathbb{C}^2$解:

$$u(x,t)=\varphi(x)+\psi(x)t+\frac{1}{2}c^2\Delta\varphi(x)t^2+\frac{1}{6}c^2\Delta\psi(x)t^3+\int_0^t[(t-\tau)f(x,\tau)+\frac{1}{6}c^2(t-\tau)^3\Delta_xf(x,\tau)]d\tau$$

证明. 先考虑问题:

$$\begin{cases} u_{tt}-c^2\Delta u=f(x,t) & \forall x\in\mathbb{R}^n, t\in\mathbb{R} \\ u=0 & \forall x\in\mathbb{R}^n, t=0 \\ u_t=0 & \forall x\in\mathbb{R}^n, t=0 \end{cases} \tag{3.2}$$

若$w(x,t;\tau)$是下面问题(3.3)的解,

$$\begin{cases} w_{tt}-c^2\Delta w=f(x,t) & \forall x\in\mathbb{R}^n, t\in(\tau,\infty) \\ w=0 & \forall x\in\mathbb{R}^n, t=\tau \\ w_t=f(x,\tau) & \forall x\in\mathbb{R}^n, t=\tau \end{cases} \tag{3.3}$$

则$u(x,t)=\int_0^t w(x,t;\tau)d\tau$是问题(3.2)的解.

没有人能把我们从康托尔为我们所创造的乐园中驱逐出去
—— 希尔伯特

令$v(x,t;\tau)=w(x,t+\tau;\tau)$,则问题(3.3)变为:

$$\begin{cases} v_{tt}-c^2\Delta v=0 & \forall x\in\mathbb{R}^n, t\in\mathbb{R} \\ v=0 & \forall x\in\mathbb{R}^n, t=0 \\ v_t=f(x,\tau) & \forall x\in\mathbb{R}^n, t=0 \end{cases} \tag{3.4}$$

由引理(2.1)可知问题(3.4)有$\mathbb{C}^2$解:

$$v(x,t;\tau)=tf(x,\tau)+\frac{1}{6}c^2t^3\Delta_x f(x,\tau),$$

从而问题(3.3)有$\mathbb{C}^2$解:

$$w(x,t;\tau)=(t-\tau)f(x,\tau)+\frac{1}{6}c^2(t-\tau)^3\Delta_x f(x,\tau),$$

从而问题(3.2)有$\mathbb{C}^2$解:

$$u(x,t)=\int_0^t[(t-\tau)f(x,\tau)+\frac{1}{6}c^2(t-\tau)^3\Delta_x f(x,\tau)]d\tau,$$

再由叠加原理及引理(2.2)知道原问题,也即问题(3.1)有$\mathbb{C}^2$解:

$$u(x,t)=\varphi(x)+\psi(x)t+\frac{1}{2}c^2\Delta\varphi(x)t^2+\frac{1}{6}c^2\Delta\psi(x)t^3+\int_0^t[(t-\tau)f(x,\tau)+\frac{1}{6}c^2(t-\tau)^3\Delta_x f(x,\tau)]d\tau.$$

□

§4 解的唯一性与稳定性

本文之前只是解决了解的存在性问题,并给出了解的一个较为简单的表达式.下面讨论问题(3.1)的解的唯一性与稳定性.

不失一般性,唯一性只用$c=1$时齐次问题:

$$\begin{cases} u_{tt}-\Delta u=0 & \forall x\in\mathbb{R}^n, t\in\mathbb{R} \\ u=0 & \forall x\in\mathbb{R}^n, t=0 \\ u_t=0 & \forall x\in\mathbb{R}^n, t=0 \end{cases} \tag{4.1}$$

只有平凡解:$u\equiv 0$.

任取点x_0及实数$R>0$,作特征锥,

$$K:\quad \| x-x_0 \|_n^2\leq (R-t)^2, 0\leq t\leq R.$$

当$t=0$时,记 $\Omega_0:\quad \| x-x_0 \|_n^2\leq R^2$.

由于锥体K是Ω_0的决定区域,故在t时刻,区域:

$$\Omega_t:\quad \| x-x_0 \|_n^2\leq (R-t)^2, 0<t<R\cdot$$

内各点的函数值$u(x,t)$由Ω_0内的初始条件完全决定,所以,Ω_t中的能量不应超过Ω_0中的能量.记

$$E(t)=\frac{1}{2}\int_{\Omega_t}(u_t^2+\| Du \|_n^2)dx=\frac{1}{2}\int_0^{R-t}dr\int_{C(x_0,r)}(u_t^2+\| Du \|_n^2)ds$$

其中,$C(x_0,r)$是在Ω_t所在的超平面上以x_0为球心,r为半径的超球面.则

$$\frac{dE(t)}{dt}=\int_{\Omega_t}(u_tu_{tt}+Du\cdot Du_t)dx-\frac{1}{2}\int_{C(x_0,R-t)}(u_t^2+\parallel Du\parallel_n^2)ds$$
$$=\int_{C(x_0,R-t)}[u_t\frac{\partial u}{\partial\overrightarrow{v}}-\frac{1}{2}(u_t^2+\parallel Du\parallel_n^2)]ds$$

而又有

$$u_t\frac{\partial u}{\partial\overrightarrow{v}}\leq\mid u_t\mid\cdot\parallel Du\parallel_n^2\leq\frac{1}{2}(u_t^2+\parallel Du\parallel_n^2)$$

故有:$\frac{dE(t)}{dt}\leq 0$,从而有$E(t)\leq E(0)=0$,于是就有$E(t)\equiv 0$.
所以在整个K中,$u_t=Du=0$,
由此可知u为常数,
即有$u(x,t)\equiv u(x,0)=0$,得证.
到这里就证明了本文中问题解的唯一性,而又定理中记得形式可知,对于任意给定的ϵ,可以找到$\delta>0$,使得只要,

$$\mid\varphi-\overline{\varphi}\mid<\delta,\mid\psi-\overline{\psi}\mid<\delta,\mid\Delta\varphi-\Delta\overline{\varphi}\mid<\delta,\mid\Delta\psi-\Delta\overline{\psi}\mid<\delta,\mid f-\overline{f}\mid<\delta,\mid\Delta_xf-\Delta_x\overline{f}\mid<\delta,$$

则在有限时间$0\leq t\leq T$内总有:$\mid u(x,t)-\overline{u}(x,t)\mid<\epsilon$. 即本文中的问题的解在有限时间内对初值和$f$都是稳定的,
也即问题的解在有限时间内是适定的.

§5　几个例子

以下几个例子都是对问题(3.1)而言的,其中n表示的是空间的维数,而$\varphi(x),\psi(x),f(x,t)$的构造也都是符合条件的,在下面例子中就不一一写出问题了.

例1: $n=1,f\equiv=0,\varphi(x)=x^2,\psi(x)=x^3$.
解:由本文的求解公式知其解为:
$u(x,t)=x^2+x^3t+c^2t^2+c^2xt^3$.
而由$d'Alembert$公式有:

$$u(x,t)=\frac{1}{2}[(x+ct)^2+(x-ct)^2]+\frac{1}{2c}\int_{x-ct}^{x+ct}y^3dy$$
$$=x^2+c^2t^2+\frac{1}{2c}\frac{1}{4}[(x+ct)^4+(x-ct)^4]$$
$$=x^2+c^2t^2+x^3t+c^2xt^3.$$

例2: $n=2,f\equiv 0,\varphi(x)\equiv 0,\psi(x)=x^5y-xy^5$.
解:由本文的求解公式知其解为:
$u(x,y;t)=(x^5y-xy^5)t+\frac{1}{6}c^2t^3(20x^3y-20xy^3)$
$=(x^5y-xy^5)t+\frac{10}{3}c^2(x^3y-xy^3)t^3$.

As for everything else, so for a mathematical theory: beauty can be perceived but not explained.
—— Arthur Cayley

而由*Poision*公式有:

$$u(x,y;t)=\frac{1}{2\pi c}\int_0^{ct}\int_0^{2\pi}\frac{(x+r\cos\theta)^5(y+r\sin\theta)-(x+r\cos\theta)(y+r\sin\theta)^5}{\sqrt{(ct)^2-r^2}}rdrd\theta$$
$$=\frac{1}{2\pi c}\int_0^{ct}\frac{y(x+r\cos\theta)^5-x(y+r\sin\theta)^5}{\sqrt{(ct)^2-r^2}}rdrd\theta$$
$$=(x^5y-xy^5)t+\frac{10}{3}c^2(x^3y-xy^3)t^3.$$

例3: $n=3, f\equiv 0, \varphi(x)\equiv 0, \psi(x)=x^3yz+xy^2z.$

解:由本文的求解公式知其解为:

$u(x,y;t)=(x^3yz+xy^2z)t+\frac{1}{3}c^2(3xyz+xz)t^3.$

而由*Kirchhoff*公式有:

$$u(x,y,z;t)$$
$$=\frac{t}{4\pi}\int_0^{2\pi}\int_0^{\pi}[(x+ct\sin\theta\cos\varphi)^3(y+ct\sin\theta\sin\varphi)(z+ct\cos\theta)$$
$$+(x+ct\sin\theta\cos\varphi)(y+ct\sin\theta\sin\varphi)^2(z+ct\cos\theta)]\sin\theta d\theta d\varphi$$
$$=\frac{t}{4}\int_0^{\pi}x(z+ct\cos\theta)[2y(x^2+y)+ct(1+3y)\sin^2\theta]\sin\theta d\theta$$
$$=\frac{t}{3}xz[3x(x^2+y)+c^2t^2(1+3y)]$$
$$=(x^3yz+xy^2z)t+\frac{1}{3}c^2(3xyz+xz)t^3.$$

例4: $n=4, f\equiv 0, \varphi(x)\equiv 0, \psi(x)=x_1^2x_2x_3x_4x_5+x_5^7.$

解:由本文的求解公式知其解为:

$u(x_1,x_2,x_3,x_4,x_5;t)=(x_1^2x_2x_3x_4x_5+x_5^7)t+\frac{1}{3}c^2(x_2x_3x_4x_5+21x_5^5)t^3.$

注: 比较可知,在符合本文条件的情况下,本文的求解公式使用起来比传统的求解公式简单得多,而且本文的求解公式还可以用于高于三阶的问题求解. 但本文所要求的条件很苛刻,这个在实际问题中很少能够碰到.

参考文献

[1] 陈祖墀,偏微分方程,第二版,中国科学技术大学出版社,2004.

对隔离定理的思考

05001 杨馨

摘 要

本文主要讨论隔离定理的变形问题,放宽隔离定理的条件,得出相应的结果.

§1 几个定义和引理

定义1.1. 拓扑向量空间:假设τ是向量空间X上分拓扑,使得
(a) X的每一点是闭集,并且,
(b) 向量空间运算关于τ是连续的.
则称τ为X上的向量拓扑,X称为拓扑向量空间.

定义1.2. 局部凸的拓扑向量空间:X是具有拓扑τ的拓扑向量空间.X是局部凸的,若存在局部基$\mathscr{B}$,它的元素都是凸的.

定义1.3. $Minkowski$泛函:$A \subset X$,A是凸的并且为吸收集,定义$\mu_A(x) = inf\{t > 0 : t^{-1}x \in A\}$,$(x \in X)$,则称$\mu_A$为$A$的$Minkowski$泛函.

引理1.1. [1] 假设K和C是拓扑向量空间X的子集,K是紧的,C是闭的,并且$K \cap C = \emptyset$,则0有邻域V,使得$(K + V) \cap (C + V) = \emptyset$.

引理1.2. 设X是拓扑向量空间.A,B是X的子集,若A是紧的,B是闭的,则$A + B$是闭的.

引理1.3. [2] 假设A是向量空间X中的凸吸收集,则
(a) $\mu_A(x + y) \leq \mu_A(x) + \mu_A(y)$,
(b) 若$t \geq 0$,则$\mu_A(tx) = t\mu_A(x)$.

---

[1] Walter Rudin,Functional Analysis, Page9, 1.10 theorem
[2] Walter Rudin,Functional Analysis, Page26, 1.35 theorem

引理1.4. [3] *Hahn − Banach*定理—控制延拓定理.假设
(a) M是实向量空间X的子空间,
(b) $p:\ X \to R$满足:对于$x \in X, y \in X, t \geq 0$,有$p(x+y) \leq p(x)+p(y), p(tx) = tp(x)$,
(c) $f:\ M \to R$是线性的,并且在M上$f(x) \leq p(x)$.
则存在线性的$\Lambda:\ X \to R$,使得$\Lambda x = f(x), (x \in M)$,并且$-p(-x) \leq \Lambda x \leq p(x), (x \in X)$.

引理1.5. [4] 设Λ是拓扑向量空间X上的线性泛函,假定对于某个$x \in X$有$\Lambda x \neq 0$,则有:
(a) Λ是连续的$\leftrightarrow$ (b) Λ在0的某个邻域中是有界的.

下面我们来证明引理(1.2),其他引理的证明见参考书目.

证明. 设$\{V_\alpha:\ \alpha \in I\}$为0点的均衡邻域基.
任取z为$A+B$的极限点,则对$\forall \alpha \in I, (z+V_\alpha) \cap (A+B) \neq \emptyset$.
设$x_\alpha + y_\alpha \in (z+V_\alpha) \cap (A+B)$,其中$x_\alpha \in A, y_\alpha \in B$.
由A的紧性知,集合$\{x_\alpha:\ \alpha \in I\}$必存在子列$\{x_m\},\ s.t.$

$$\lim_{m\to\infty} x_m = x_0,\ x_0 \in A.$$

相应的均衡邻域记为$\{V_m:\ m = 1, 2, \cdot, n, \cdot\}$.
任取0点的邻域W,存在均衡邻域V,使得$V+V \subset W$.
因为

$$\lim_{m\to\infty} x_m = x_0,$$

所以$\exists N$,当$n \geq N$时,有$x_n \in x_0 + V$,
即$z - x_n \in z - x_0 + V$.
$\exists n_0 \geq N, s.t.\ V_{n_0} \subset V$,有$x_{n_0} + y_{n_0} \in z + V_{n_0}$,即$y_{n_0} \in z - x_{n_0} + V_{n_0}$.
故有$y_{n_0} \in z - x_{n_0} + V_{n_0} \subset z - x_0 + V_{n_0} + V$.
从而有$y_{n_0} \in z - x_0 + V_{n_0} + V \subset z - x_0 + V + V \subset z - x_0 + W$,
又$y_{n_0} \in B$,所以$y_{n_0} \in (z - x_0 + W) \cap B$.
即对0的任何邻域W,$z - x_0 + W$与B的交不空.
所以$z - x_0 \in \overline{B} = B$,
从而$\exists y_0 \in B, s.t.\ z = x_0 + y_0$,即$z \in (A+B)$,
从而$A+B$是闭集.

□

§2 主要结果—隔离定理的扩充

定理5. 假设A和B是拓扑向量空间X中的不相交凸集,A是紧的,B是闭的,并且$\mathring{A}, \mathring{B} \neq \emptyset$.则$\exists \Lambda \in X^*, \gamma_1 \in \mathbf{R}, \gamma_2 \in \mathbf{R}$,使得对每个$x \in A$和每个$y \in B, Re\Lambda x < \gamma_1 < \gamma_2 < Re\Lambda y$.

[3] Walter Rudin,Functional Analysis, Page56, 3.2 theorem
[4] Walter Rudin,Functional Analysis, Page14, 1.18 theorem

证明. 只要对实标量域证明即可.
若实的情况成立,当标量域为C时,取实线性的Λ_1所对应的唯一的复线性泛函Λ即可.
现在假设标量域是实的.
固定$a_0 \in \overset{\circ}{A}, b_0 \in \overset{\circ}{B}$,令$x_0 = b_0 - a_0, C = A - B + x_0$;
由引理(1.2)知C为闭的,并且由A, B的凸性知C为凸的,$\overset{\circ}{C}$是X中0的凸邻域.
设p是C的$Minkowski$泛函,由引理(1.3)知,p满足引理(1.4)的条件$(a), (b)$.
因为$A \cap B = \emptyset, x_0 \notin C$,故$p(x_0) \geq 1$.
又C是闭的,由引理(1.1)知,$\exists 0$的邻域$V, s.t.\ (x_0 + V) \cap C = \emptyset$.从而$p(x_0) > 1$.
在由x_0生成的X的子空间M上定义$f(tx_0) = t(1 + \varepsilon)$,
其中$1 + \varepsilon \leq p(x_0), \varepsilon > 0$.
若$t \leq 0$,则$f(tx_0) = t(1 + \varepsilon) \leq tp(x_0) = p(tx_0)$.
若$t < 0$,则$f(tx_0) < 0 \leq p(tx_0)$,于是在M上有$f \leq p$.
由引理(1.4),f可以延拓为X上的线性泛函Λ,仍满足$\Lambda \leq p$.
特别地,在C上,$\Lambda \leq 1$,从而在$-C$上$\Lambda \geq -1$,所以在$C \cap (-C)$上$|\ \Lambda\ | \leq 1$.
从而在0的邻域$\overset{\circ}{C} \cap (-\overset{\circ}{C})$上$|\ \Lambda\ | \leq 1$.
由引理(1.5)知$\Lambda \in X^*$.
$\forall a \in A, b \in B$,因为$\Lambda x_0 = 1 + \varepsilon, a - b + x_0 \in C$.$C$是闭的,所以
$\Lambda a - \Lambda b + 1 + \varepsilon = \Lambda(a - b + x_0) \leq p(a - b + x_0) \leq 1$.
故有$\Lambda a + \epsilon \leq \Lambda b$,从而

$$\sup_{a \in A} \Lambda a + \epsilon \leq \inf_{b \in B} \Lambda b$$

令

$$\gamma_1 = \sup_{a \in A} \Lambda a + \frac{\epsilon}{4}, \gamma_2 = \sup_{a \in A} \Lambda a + \frac{\epsilon}{2}.$$

则有
$\Lambda a < \gamma_1 < \gamma_2 < \Lambda b, \forall a \in A, b \in B$.

□

参考文献

[1] Walter Rudin,Functional Analysis

God exists since mathematics is consistent, and the Devil exists since we cannot prove it.

—— Andre Weil

关于Vine and pair-copula method

05017 沈娟

§1 引出原因

在实际中有大量的高维数据,然而一般这些高维数据并没有一个统一的清晰的表达.虽然多元正态有着众多良好的性质:对线性运算封闭,有统一形式等等,但是很多问题不能归于正态分布.

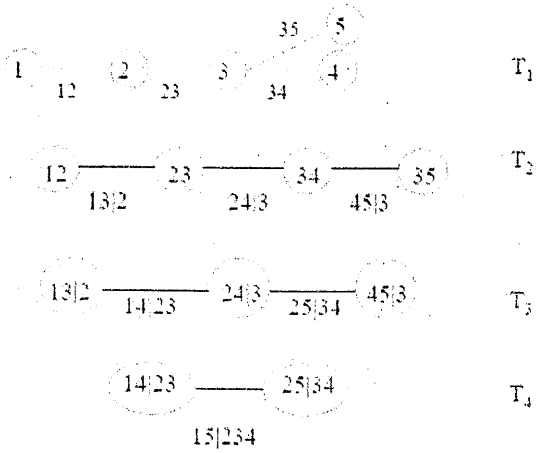
虽然对高维数据建模是比较困难的,但是每个变量的边缘分布还是比较容易估计的.如果边缘分布都已经知道,用copula就可以得到其它分布.但高维的copula也是难以处理的,因此可以先把密度分解为二维的形式.这样就比较容易建立实际模型进行分析了. 这种概率构建方法展现了一种崭新的方法来构造复杂多元相关结构模型,关键是利用基于条件独立的简单构造模块来对相关结构进行建模.

§2 概念和相关定理

1.vine

Vine是一种图形结构.N个变量的vine:第j个树的边是第j+1个树的顶点,j=1,…,N-2,并且每棵树的边数达到最大.

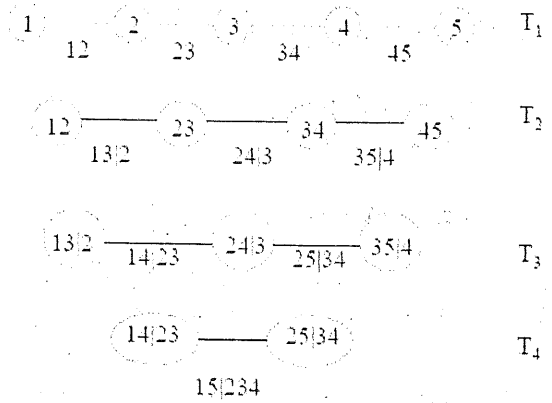
一个vine的某一条边的constraint,conditioned和conditioning sets分别是指:形成这一条边所要涉及到的所有变量集;这条边的两个端点的constraint sets的不同变量部分,这条边的两个端点的constraint sets的相同变量部分.



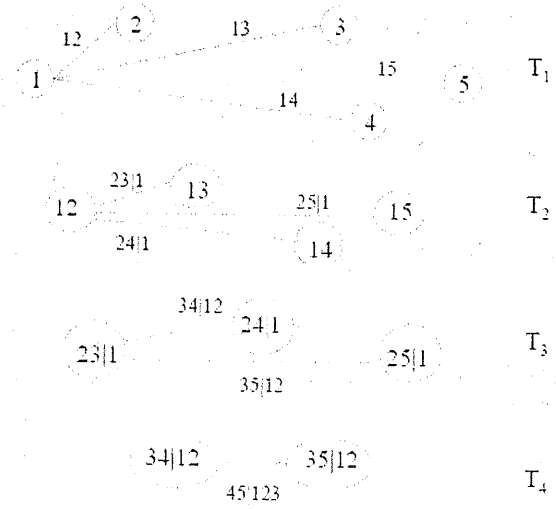
N个变量的regular vine是指第j棵树的两条边如果有公共顶点,则在第j+1棵树中由一条边相连接.这样一个有N个变量的regular vine必然有N(N-1)/2条边.

还有两个特殊的regular vine: D-vine和canonical-vine(C-vine).

D-vine是指任何一个顶点的度都不超过2的vine;



C-vine是指每第i棵树都有且仅有一个度为(N-i)的顶点的vine.



2,copula

copula是指边缘分布为U(0,1)的多维分布, 运用copula可以将联合分布函数分为两部分内容: 单个变量边缘分布和变量间相关结构。

根据Sklar定理,任何一个$d(d \geq 2)$维的分布函数F对应一个copula C:

$F(x) = C(F_1(x_1), \cdots, F_d(x_d)), x \in \mathbf{R}^d$

若F连续并且对应边缘分布$F_1, f_2, \cdots, F_d$, 那么有:

$C(a_1, \cdots, a_n) = F(F_1^{-1}(a_1), \cdots, F_d^{-1}(a_d)), x \in \mathbf{R}^d$,并且此时C唯一.

对于密度函数有:

$$p(x) = \frac{\partial^d F(x)}{\partial x_1 \cdots \partial x_d} = \frac{\partial^d C(a)}{\partial x_1 \cdots \partial x_d} = \frac{\partial^d C(a)}{\partial a_1 \cdots \partial a_d} \prod_{\nu \in \upsilon} \frac{\partial a_\nu}{\partial x_\nu} = c(a) \prod_{\nu \in \upsilon} p_\nu(x_\nu)$$

****

Almost all new ideas have a certain aspect of foolishness when they are first produced.

—— Alfred North Whitehead

其中c(a)为C对应的copula密度函数:$c(a)=\frac{\partial^d C(a)}{\partial x_1\cdots\partial x_d}$.

例如二元Gaussian copula

$$C_\rho(u_1,u_2)=\iint\limits_{\substack{s\le\Phi^{-1}(u_1)\\ t\le\Phi^{-1}(u_2)}}\frac{1}{2\pi(1-\rho^2)^{(1/2)}}exp\{\frac{-(s^2-2\rho st+t^2)}{2(1-\rho^2)}\}dsdt$$

对应的density为:

$$c_\rho(s,t)=\frac{1}{(1-\rho^2)^{(1/2)}}exp\{\frac{-\rho^2(s^2+t^2)-2\rho st}{2(1-\rho^2)}\}$$

3, 对任意的随机变量X,服从分布F,令$F^{-1}(\alpha)=\inf\{x|F(x)\ge\alpha\},\alpha\in(0,1)$,则有:

(1)对任意服从U(0,1)的随机变量U,$F^{-1}(U)\sim F$

(2)设F连续,那么有$F(X)\sim U(0,1)$

对高维情况有:

(1)若$(X_1,\cdots,X_n)$服从分布F,且F绝对连续,那么

$U_1=F_1(X_1),U_2=F_{2|1}(X_2|X_1),\cdots,U_n=F_{n|1\cdots n-1}(X_n|X_1,\cdots,X_{n-1}),iid\sim U(0,1)$

(2)若$U_1,\cdots,U_n,iid\sim U(0,1)$,令

$$\begin{cases}X_1=U_1,\\ X_2=F^{-1}(U_2|X_1),\\ \quad\vdots\\ X_n=F^{-1}(U_n|X_1,\cdots,X_{n-1})\end{cases}$$

则$(X_1,\cdots,X_n)\sim F$.

§3 前期工作

1,将一般密度函数分解为pair-copula

考虑随机向量$(X_1,\cdots,X_n)$,密度函数可展成:

$f(x_1,\cdots,x_n)=f_n(x_n)\cdot f(x_{n-1}|x_n)\cdot f(x_{n-2}|x_{n-1},x_n)\cdots f(x_1|x_2,\cdots,x_n)$

结合copula有:

$f(x_1,\cdots,x_n)=c_{1\cdots n}\{F_1(x_1),\cdots,F_n(x_n)\}\cdot f_1(x_1)\cdots f_n(x_n)$

N=2时,有$f(x_1,x_2)=c_{12}\{F_1(x_1),F_2(x_2)\}\cdot f_1(x_1)\cdot f_2(x_2)$

从而$f(x_1|x_2)=c_{12}\{F_1(x_1),F_2(x_2)\}\cdot f_1(x_1)$

进而$f(x_1|x_2,x_3)=c_{12|3}\{F(x_1|x_3),F(x_2|x_3)\}\cdot f_1(x_1|x_3)$

同样地,有$f(x_1|x_2,x_3)=c_{13|2}\{F(x_1|x_2),F(x_3|x_2)\}\cdot f_1(x_1|x_2)$

再分解$f(x_1|x_2)$可得:

$f(x_1|x_2,x_3)=c_{13|2}\{F(x_1|x_2),F(x_3|x_2)\}\cdot c_{12}\{F(x_1),F(x_2)\}\cdot f_1(x_1)$

依次类推,我们就可以将原密度函数分解为pair-copula和边缘密度的乘机,对于3维结果如下:

$f(x_1,x_2,x_3) = c_{13|2}\{F(x_1|x_2),F(x_3|x_2)\}\cdot c_{12}\{F_1(x_1),F_2(x_2)\}\cdot c_{23}\{F_3(x_3),F_2(x_2)\}\cdot f_1(x_1)\cdot f_2(x_2)\cdot f_3(x_3)$

对于更高维情况,选择变量的顺序不一样,会影响表达形式.为了简便,对于特定的vine,通常把conditioning variables 尽量向后排.

比如4维时,对于C-vine密度函数可以写为:

$f(x_1,x_2,x_3,x_4) = f_1(x_1)\cdot f_2(x_2)\cdot f_3(x_3)\cdot f_4(x_4)\cdot c_{12}\{F_1(x_1),F_2(x_2)\}\cdot c_{13}\{F_1(x_1),F_3(x_3)\}\cdot c_{14}\{F_1(x_1),F_4(x_4)\}\cdot c_{23|1}\{F(x_2|x_1),F(x_3|x_1)\}\cdot c_{24|1}\{F(x_2|x_1),F(x_4|x_1)\}\cdot c_{34|12}\{F(x_3|x_1,x_2),F(x_4|x_1,x_2)\}$

而对于D-vine,有

$f(x_1,x_2,x_3,x_4) = f_1(x_1)\cdot f_2(x_2)\cdot f_3(x_3)\cdot f_4(x_4)\cdot c_{12}\{F_1(x_1),F_2(x_2)\}\cdot c_{23}\{F_3(x_3),F_2(x_2)\}\cdot c_{34}\{F_3(x_3),F_4(x_4)\}\cdot c_{13|2}\{F(x_1|x_2),F(x_3|x_2)\}\cdot c_{24|3}\{F(x_2|x_3),F(x_4|x_3)\}\cdot c_{14|23}\{F(x_1|x_2,x_3),F(x_4|x_2,x_3)\}$

更高维情况,易得

$$f(x|\nu) = c_{x\nu_j|\nu_{-j}}\{F(x|\nu_{-j}),F(\nu_j|\nu_{-j})\cdot f(x|\nu_{-j})\}$$

其中ν为随机向量,ν_j为ν的任一维变量,而ν_{-j}是原向量去掉这一变量得到的向量.这样任一密度都可以拆为pair-copula与边缘密度乘机的形式.

Joe(1996)给出

$$F(x|\nu) = \frac{\partial c_{x\nu_j|\nu_{-j}}\{F(x|\nu_{-j}),F(\nu_j|\nu_{-j})\}}{\partial F(\nu_j|\nu_{-j})}$$

特别地,如果v为一维,上式变为:

$$F(x|\nu) = \frac{\partial C_{x\nu}\{F(x),F(\nu)\}}{\partial F(\nu)}$$

当x,v为均匀分布随机变量时,表示为:

$h(x,\nu,\Theta) = F(x|\nu) = \frac{\partial C_{x\nu}(x,\nu,\Theta)}{\partial \nu}$,($\Theta$为参数集)

后面还会用到h^{-1},指这里的函数h对第一个变量ν求逆.

比如前面提到的二维Gaussian copula,有

$h(u_1,u_2,\rho) = \Phi\left(\frac{\Phi^{-1}(u_1)-\rho\Phi^{-1}(u_2)}{\sqrt{1-\rho^2}}\right)$

$h_{12}^{-1}(u_1,u_2,\rho) = \Phi\{\Phi^{-1}(u_1)\sqrt{1-\rho^2}+\rho\Phi^{-1}(u_2)\}$

对两个特殊的vine,有分解式:

$$D-vine: \prod_{k=1}^{n} f(x_k)\prod_{j=1}^{n-1}\prod_{i=1}^{n-j} c_{i,i+j|i+1,\cdots,i+j-1}\{F(x_i|x_{i+1},\ldots,x_{i+j+1}),F(x_{i+j}|x_{i+1},\cdots,x_{i+j-1})\}$$

$$C-vine: \prod_{k=1}^{n} f(x_k)\prod_{j=1}^{n-1}\prod_{i=1}^{n-j} c_{j,i+j|1,\cdots,j-1}\{F(x_j|x_1,\ldots,x_{j-1}),F(x_{i+j}|x_1,\cdots,x_{j-1})\}$$

****

God may not play dice with the universe, but something strange is going on with the prime numbers.

—— Paul Erdos

2,条件独立和pair-copula

假设条件独立可以减少pair-copula分解式层次的数目，从而简化构建过程.

比如在三维条件下,原来有

$f(x_1,x_2,x_3) = c_{13|2}\{F(x_1|x_2),F(x_3|x_2)\}\cdot c_{12}\{F_1(x_1),F_2(x_2)\}\cdot c_{23}\{F_3(x_3),F_2(x_2)\}\cdot f_1(x_1)\cdot f_2(x_2)\cdot f_3(x_3)$

若x_1,x_2关于x_3条件独立,那么$c_{13|2}\{F(x_1|x_2),F(x_3|x_2)\}=1$,这是由于$\frac{\partial^2(st)}{\partial s\partial t}=1$

上式可简化为:$f(x_1,x_2,x_3)=c_{12}\{F_1(x_1),F_2(x_2)\}\cdot c_{23}\{F_3(x_3),F_2(x_2)\}\cdot f_1(x_1)\cdot f_2(x_2)\cdot f_3(x_3)$

一般地,若x,y给定随机变量ν条件独立,则有$c_{xy|\nu}\{F(x|\nu),F(y|\nu)\}=1$

上式中,如果我们假定x_1,x_2关于x_3条件独立,产生的误差将为$c_{13|2}\{F(x_1|x_2),F(x_3|x_2)-1\}$

其它情况类似.

§4 Sampling

根据定理:若$U_1,\cdots,U_n,iid\sim U(0,1)$,令

$$\begin{cases} X_1 = U_1, \\ X_2 = F^{-1}(U_2|X_1), \\ \quad\cdots \\ X_n = F^{-1}(U_n|X_1,\cdots,X_{n-1}) \end{cases}$$

则$(X_1,\cdots,X_n)\sim F$.

我们构造高维vine时,只需令

$$\begin{cases} x_1 = u_1, \\ x_2 = F^{-1}(u_2|x_1), \\ \quad\vdots \\ x_n = F^{-1}(u_n|x_1,\cdots,x_{n-1}) \end{cases}$$

对于n维C-vine,我们选择:

$$F(x_j|x_1,\cdots,x_{j-1}) = \frac{\partial C_{j,j-1|1,\cdots,j-2}\{F(x_j|x_1,\cdots,x_{j-2}),F(x_{j-1}|x_1,\cdots,x_{j-2})\}}{\partial F(x_{j-1}|x_1,\cdots,x_{j-2})}$$

令$\nu_{i,j}=F(x_j|x_1,\cdots,x_{j-1})$,$\Theta_{j,i}$表示$c_{j,j+i|1,\cdots,j-1}$中的参数集,

即$\nu_{j,j}=h(\nu_{j,j-1},\nu_{j-1,j-1},\Theta_{j,1})$

从而得到n维C-vine的算法为:

首先sample n 个(0,1)上独立随机变量$u_1,u_2,\cdots,u_n$

$x_1=\nu_{1,1}=u_1$

$for\quad i\leftarrow 2,\cdots,n$

$\nu_{i,1}=u_i$

for $k \leftarrow i-1, i-2, \cdots, 1$
$\nu_{i,1} = h^{-1}(\nu_{i,1}, \nu_{k,k}, \Theta_{k,j-k})$
end for
$x_i = \nu_{i,1}$
if $i == n$ *then*
Stop
end if
for $j \leftarrow 1, \cdots, i-1$
$\nu_{i,j+1} = h(\nu_{i,j}, \nu_{j,j}, \Theta_{k,j-k})$
end for
end for
对于n维D-vine,选择

$$F(x_j|x_1, \cdots, x_{j-1}) = \frac{\partial C_{j,1|2,\cdots,j-1}\{F(x_j|x_2, \cdots, x_{j-1}), F(x_1|x_2, \cdots, x_{j-1})\}}{\partial F(x_1|x_2, \cdots, x_{j-1})}$$

令$\Theta_{j,i}$表示$c_{j,j+i|i+1,\cdots,i+j-1}$中的参数集,
$\nu_{i,2j} = F(x_{i-j}|x_{i-j+1}, \cdots, x_i); \nu_{i,2j+1} = F(x_i|x_{i-j}, \cdots, x_{i-1})$
同样的,得到n维D-vine的算法:
首先sample n 个(0,1)上独立随机变量$u_1, u_2, \cdots, u_n$
$x_1 = \nu_{1,1} = u_1$
$x_2 = \nu_{2,1} = h^{-1}(u_2, \nu_{1,1}, \Theta_{1,1})$
$\nu_{2,2} = h(\nu_{1,1}, \nu_{2,1}, \Theta_{1,1})$
for $i \leftarrow 3, \cdots, n$
$\nu_{i,1} = u_i$
for $k \leftarrow i-1, i-2, \cdots, 2$
$\nu_{i,1} = h^{-1}(\nu_{i,1}, \nu_{i-1,2k-2}, \Theta_{k,i-k})$
end for
$\nu_{i,1} = h^{-1}(\nu_{i,1}, \nu_{i-1,1}, \Theta 1, i-1)$
$x_i = \nu_{i,1}$
if $i == n$ *then*
Stop
end if
$\nu_{i,2} = h(\nu_{i-1,1}, \nu_{i,1}, \Theta_{1,i-1})$
$\nu_{i,3} = h(\nu_{i,1}, \nu_{i-1,1}, \Theta_{1,i-1})$
if $i > 3$ *then for* $j \leftarrow 2, \cdots, i-2$
$\nu_{i,2j} = h(\nu_{i-1,2j-2}, \nu_{i,2j-1}, \Theta_{j,i-j})$
$\nu_{i,2j+1} = h(\nu_{i,2j-1}, \nu_{i-1,2j-2}, \Theta_{j,i-j})$
end for
end if
$\nu_{i,2i-2} = h(\nu_{i-1,2i-4}, \nu_{i,2i-3}, \Theta_{i-1,1})$

It is impossible to be a mathematician without being a poet in soul.
—— Sofia Kovalevskaya

end for

例如构造3维vinc
首先构造3个独立的服从U(0,1)的u_1, u_2, u_3
令$x_1 = u_1$,我们有$F(x_2|x_1) = h(x_2, x_1, \Theta_{11})$,从而$x_2 = h^{-1}(u_2, x_1, \Theta_{11})$
又有$F(x_3|x_1, x_2) = h(h(x_3, x_1, \Theta_{12}), h(x_2, x_1, \Theta_{11}), \Theta_{21})$,
从而$x_3 = h^{-1}[h^{-1}(u_3, h(x_2, x_1, \Theta_{11}), x_1, \Theta_{12}]$

§5 Inference

对于给定的vine,可以写出似然函数,进一步进行参数估计.
对于C-vine,对数似然函数为: (以下T为观察次数)

$$\sum_{j=1}^{n-1}\sum_{i=1}^{n-j}\sum_{t=1}^{T}\log[c_{j,j+i|1,\cdots,j-1}\{F(x_{j,t}|x_{1,t},\cdots,x_{j-1,t}), F(x_{j+i,t}|x_{1,t},\cdots,x_{j-1,t})\}]$$

令$\nu_{j,i,t} = F(x_{i+j,t}|x_{1,t},\cdots,x_{j,t})$, $L(x,\nu,\Theta) = \sum_{t=1}^{T}\log[c(x_t,\nu_t,\Theta)]$
从而得到计算C-vine的对数似然函数的算法为:
$log - likelihood = 0$
$for \quad i \leftarrow 1,\cdots,n$
$\nu_{0,i} = x_i$
end for
$for \quad j \leftarrow 1,\cdots,n-1$
$for \quad i \leftarrow 1,\cdots,n-j$
$log - likelihood = loglikelihood + L(\nu_{j-1,1}, \nu_{j-1,i+1}, \Theta_{j,i})$
end for
$if\ j == n-1 \quad then$
Stop
end if
$for \quad i \leftarrow 1.\cdots,n-j$
$\nu_{j,i} = h(\nu_{j-1,i+1}, \nu_{j-1,1}, \Theta_{j,i})$
end forend for

而D-vine,对数似然函数为:

$$\sum_{j=1}^{n-1}\sum_{i=1}^{n-j}\sum_{t=1}^{T}\log[c_{j,j+i|i+1,\cdots,i+j-1}\{F(x_{i,t}|x_{i+1,t},\cdots,x_{i+j-1,t}), F(x_{j+i,t}|x_{i+1,t},\cdots,x_{i+j-1,t})\}]$$

令$\Theta_{j,i}$表示$c_{i,j+i|i+1,\cdots,i+j-1}$中的参数集
则得到计算D-vine的对数似然函数的算法:

$log-likelihood=0$
$for\ i=1,\cdots,n$
$\nu_{0,i}=x_i$
$end\ for$
$for\quad i\leftarrow 1,\cdots,n-1$
$log-likelihood=loglikelihood+L(\nu_{0,i},\nu_{0,i+1},\Theta_{1,i})$
$end\ for$
$\nu_{1,1}=h(\nu_{0,1},\nu_{0,2},\Theta_{1,1})$
$for\quad k=1,\cdots,n-3$
$\nu_{1,2k}=h(\nu_{0,k+2},\nu_{0,k+1},\Theta_{1,k+1})$
$\nu_{1,2k+1}=h(\nu_{0,k+1},\nu_{0,k+2},\Theta_{1,k+1})$
$end\ for$
$\nu_{1,2n-4}=h(\nu_{0,n},\nu_{0,n-1},\Theta_{1,n-1})$
$for\quad j=2,\cdots,n-1$
$for\quad i=1,\cdots,n-j$
$log-likelihood=loglikelihood+L(\nu_{j-1,2i-2},\nu_{j-1,2i},\Theta_{j,i})$
$end\ for$
$if\ j==n-1\quad then$
$Stop$
$end\ if$
$\nu_{j,1}=h(\nu_{j-1,1},\nu_{j-1,2},\Theta_{j,1})$
$if\ n>4\quad then$
$for\quad i=1,2,\cdots,n-j-2$
$\nu_{j,2i}=h(\nu_{j-1,2i+2},\nu_{j-1,2i+1},\Theta_{j,i+1})$
$\nu_{j,2i+1}=h(\nu_{j-1,2i+1},\nu_{j-1,2i+2},\Theta_{j,i+1})$
$end\ for$
$end\ if$
$\nu_{j,2n-2j-2}=h(\nu_{j-1,2n-2j},\nu_{j-1,2n-2j-1},\Theta_{j,n-j})$
$end\ for$

例如三维情况下,对数似然函数可写为

$$\sum_{t=1}^{T}\{\log c_{12}(x_{1,t},x_{2,t},\Theta_{11})+\log c_{23}(x_{2,t},x_{3,t},\Theta_{12})+\log c_{13|2}(x_{1,t},x_{2,t},\Theta_{21})\}$$

因此:$\nu_{1,t}=F(x_{1,t}|x_{2,t})=h(x_{1,t},x_{2,t},\Theta_{11})$
$\nu_{2,t}=F(x_{3,t}|x_{2,t})=h(x_{3,t},x_{2,t},\Theta_{12})$
得到极大似然函数后就可以所有参数进行数值最大化估计。

§6 拟合优度检验

令$X_1,\cdots,X_n$是边缘分布分别为$F(x_i)$的随机向量,令

$T(X_1)=F_1(x_1)$,

$T(X_2)=F_{2|1}(x_2|x_1)$,

$\cdots$,

$T(X_n)=F_{n|1,\cdots,n-1}(x_n|x_1,\cdots,x_{n-1})$,

如果数据拟合得好,应有$T(X_1),\cdots,T(X_n),iid\sim U(0,1)$,令$Z_i=T(X_i)$.

接下来只需检验$T(X_1),\cdots,T(X_n),iid\sim U(0,1)$

可以令$S=\sum_{i=1}^{n}\{\phi^{-1}(Z_i)\}^2$,再检验S是否为自由度为n的卡方即可.

对C-vine 的检验的转化的算法如下:

for $t\leftarrow 1,\cdots,T$

$z_{1,t}=x_{1,t}$

for $i\leftarrow 2,\cdots,n$

$z_{i,t}=x_{i,t}$

for $j\leftarrow 1,\cdots,i-1$

$z_{i,t}=h(z_{i,t},z_{j,t},\Theta_{j,i-j})$

end for

end for

end for

§7 结论

通过一组pair-copula对多元联合分布进行分解，分解成边缘分布和一组pair-copula函数的乘积,使对高维数据的估计大大简化。但是对copula事先的选择范围和拟合优度检验的合理性等都有待进一步强化.

Some Discussions on Coin Tossing Problem

05017 王威 *05001 杨熠*

In the course of Stochastic Processes, we often come across problems arising in tossing coins. As we find this kind of problems very interesting, we attempt to make a generalization from a simple case. During this process, we employ some high-level notions and techniques that we learnt in Stochastic Processes course and being able to apply the knowledge really makes us encouraged.

Original Problem: *In a fair coin tossing game, the game stops when r heads appear consecutively. What is the expected number to flip the coin until the game stops?*

Solution:(A standard approach) Let T_r denote the number of tossing when the first r consecutive heads appears. Let $P_n \triangleq \mathbf{Pr}(T_r = n), P_n^* \triangleq \mathbf{Pr}(T_r > n)$, and it is easy to show that $P_i = 0$, for $0 \leq i \leq r-1$, and $P_r = 1/2^r$. From the fact that $P_{n+r+1} = P_n^* \times 1/2 \times 1/2^r$. Then it establishes that

$$\mathbf{E}T_r = \sum_{n=0}^{\infty} \mathbf{Pr}(T_r > n) = \sum_{n=0}^{\infty} P_n^* = \sum_{n=0}^{\infty} 2^{r+1} P_{n+r+1} = 2^{r+1}(1 - \sum_{n=0}^{r} P_n) = 2^{r+1} - 2$$

Hints for generalization:
This is a quite standard and easy case. However, we can generalize it to more extended form. There are actually three points that we can make generalization: **i)**In stead of two outcomes in coin tossing, the experiment can have n outcomes; **ii)**In stead of a fair game, different outcomes can have different possibilities; **iii)** We can also change the stopping rule in two ways. First, the stop pattern can be more general, for example, HTHTHT. Second, In stead of stopping when r consecutive heads appears, the stopping rule can be changed to when either r consecutive heads or tails appears, or in generalized case, when any outcome appears r times consecutively.

It is easy to see that if we only change the first and second point, which means a multi-outcome unfair game but with the same stopping rule, the almost unchanged method can be applied to solve this problem. So the really interesting part comes when we change the stopping rule.

First, we discuss the case of generalized stopping pattern.

Case 1 (Generalized stopping pattern version)

Problem: *In fair coin tossing game, the game stops when the pattern HTHT appears. What is the expected number to flip the coin until the game stops?*

Solution: To solve this problem, we should use the notion of Renewal Processes and the famous *Blackwell Theorem* (See Appendix). Assuming that the tossing would last infinitively, we define that a renewal happens when the pattern HTHT appears. Let X_i denotes the outcome of the ith toss and T_i denotes the number of tosses from the $(i-1)$th renewal to the ith renewal, then we have a Delayed Renewal Processes, in which, T_i, $i \geq 2$, follow the same distribution while T_1 follows a different one. It is because T_i, $i \geq 2$, actually denotes the number of tosses to have pattern HTHT conditioned on HT, while T_1 denotes the number of tosses to have pattern HTHT with no conditions.

By *Blackwell Theorem* we have

$$\begin{aligned}\mathbf{E}T_2 &= (\lim_{n\to\infty} \mathbf{Pr}(\textit{Pattern happens at the nth toss}))^{-1} \\ &= (\mathbf{Pr}(X=H)\mathbf{Pr}(X=T)\mathbf{Pr}(X=H)\mathbf{Pr}(X=T))^{-1} \\ &= 2^4 = 16\end{aligned}$$

Then for solving $\mathbf{E}T_1$, define T^* as the number of tosses when pattern HT appears, we notice that $T_1 = T^* + T_2$. Because the pattern HT doesn't have repetition in its structure (that is the fundamental difference between the patterns), applying the same method above we obtain $\mathbf{E}T^* = 4$. Thus it establishes that

$$\mathbf{E}T_1 = \mathbf{E}T^* + \mathbf{E}T_2 = 16 + 4 = 20$$

Remark. **i)** The method is easy to be applied to patterns with more complicated repetitive structure, such as HTHTHT, and in particular, r consecutive heads. In that case, it is easy to verify that the expectation of number of tosses is $\sum_{i=1}^{r} 2^i = 2^{r+1} - 2$, which is the same with the result of the original problem. **ii)**The method can be applied to the case of multi-outcome unfair game easily.

Then let's talk about another stopping rule. **In the discussion below, we assume that the game stops when any outcome appeared r times consecutively.**

Case 2 (Multi-outcome fair game version)

Problem: *Now we assume that in a repeated experiment with n outcomes, each outcome appears with a probability of $1/n$. What is the expected number of trials until the experiment stops?*

Analysis: At first glance, this case is much more difficult as the stopping rule involves all the outcomes. But we can notice that if we now have a particular outcome appearing m times consecutively, after the next trial, the probability that we obtain $m+1$ consecutive outcome is $\frac{1}{n}$, while the probability that we will start from a different outcome (which appear 1 time) is

$\frac{n-1}{n}$. So this problem can be solved by establishing a Markov Chain model.

Solution: The Markov Chain is like this: $S = \{S_1, S_2 \dots S_r\}$ denotes the sets of states, while the chain is in state S_i when the latest run of consecutive outcomes has a length of i; X_n denotes the state after n trials. Then we have a Markov Chain with transition probability

$$P_{i,1} = \frac{n-1}{n}, P_{i,i+1} = \frac{1}{n}, \qquad 1 \le i < r,$$
$$P_{r,r} = 1.$$

Let T_i denotes the number of trials needed to first reach state S_i. It is obvious that the chain will reach state S_{i-1} before it reaches S_i, so conditioned on the first trial after the chain first reaches state S_{i-1}, we obtain that

$$\begin{aligned}\mathbf{E}T_i &= P_{i-1,i}\mathbf{E}[T_i|S_{i-1} \to S_i] + P_{i,1}\mathbf{E}[T_i|S_{i-1} \to S_1] \\ &= \frac{1}{n}(1 + \mathbf{E}T_{i-1}) + \frac{n-1}{n}(\mathbf{E}T_{i-1} + \mathbf{E}T_i), \qquad 2 \le i \le r\end{aligned}$$

and boundary condition

$$\mathbf{E}T_1 = 1$$

Then it establishes that

$$\mathbf{E}T_r = 1 + n\mathbf{E}T_{r-1} = \cdots = \sum_{i=0}^{r-1} n^i$$

When n=2, we have

$$\mathbf{E}T_r = \sum_{i=0}^{r-1} 2^i = 2^r - 1$$

And it is interesting to notice that it is one half of the result of the original problem.

Case 3 (Two-outcome unfair game version)

Problem: *Now we assume a unfair coin tossing game, the probability of a head is* $p, 0 < p < 1$, *What is the expected number to flip the coin until the game stops?*

Analysis: The heterogeneity of the outcomes makes the Markov Chain model unapplicable. We have to solve it with more elaborate conditional probability techniques.

Solution: Let T_r denotes the number of tosses before the game stops and H denotes the

God made integers, all else is the work of man.
—— Leopold Kronecker

number of tosses when the first head appears, and T denotes the number of tosses when first tail appears. Then it establishes that

$$\begin{aligned}\mathbf{E}T_r &= \sum_{i=1}^{r}\mathbf{Pr}(H=i)\mathbf{E}[T_r|H=i] + \mathbf{Pr}(H>r)\mathbf{E}[T_r|H>r] \\ &= \sum_{i=0}^{r} p(1-p)^{i-1}(i-1+\mathbf{E}[T_r|H=1]) + (1-p)^r r \\ &= \sum_{i=0}^{r}(1-p)^i + [1-(1-p)^r]\mathbf{E}[T_r|H=1]\end{aligned}$$

Similarly, we have

$$\mathbf{E}T_r = \sum_{i=0}^{r} p^i + [1-p^r]\mathbf{E}(T_r|T=1)$$

Conditioned on the first toss, we obtain

$$\begin{aligned}\mathbf{E}T_r &= \mathbf{Pr}(H=1)\mathbf{E}[T_r|H=1] + \mathbf{Pr}(T=1)\mathbf{E}[T_r|T=1] \\ &= p\mathbf{E}[T_r|H=1] + (1-p)\mathbf{E}[T_r|T=1]\end{aligned}$$

Solving the three equations we have

$$\mathbf{E}T_r = [\frac{p}{1-(1-p)^r} + \frac{1-p}{1-p^r} - 1]^{-1}$$

When the game is fair, i.e.$p = 1/2$, we have

$$\mathbf{E}T_r = 2^r - 1$$

Again, the result is one half of that of the original problem.

Case 4 (Multi-outcome unfair game version)

Problem: *Now we assume that in a repeated experiment with n outcomes, the ith outcome appears with a probability of* p_i $(\sum_{i=1}^{n} p_i = 1)$. *What is the expected number of trials until the experiment stops?*

Unfortunately, we still haven't solved this most generalized version. We leave it as an open problem.

Appendix

Delayed Renewal Processes and Blackwell Theorem

$\{T_n,\ n = 1,2,3\ldots\}$ is a sequence of independent nonnegative random variables, T_1 follows distribution F and T_i follows distribution G, $i > 2$. Let

$$N_D(t) \triangleq sup\{n:\ S_n \le t\}$$

Then $N_D(t)$ is a *Delayed Renewal Process*. Distribution F is latticed if the corresponding random variable X satisfy $\mathbf{Pr}(X = nd) = 1$, for a certain $d \neq 0$, and d is the period of the distribution. And the *Blackwell Theorem* states that if F and G are latticed with period d, then

$$\lim_{n\to\infty} \mathbf{E}[numbers\ of\ renewals\ at\ time\ nd] = \frac{d}{\mathbf{E}T_2}$$

Because T_2's distribution is latticed with period 1, and at any time there is at most one renewal, so it follows that

$$\mathbf{E}T_2 = (\lim_{n\to\infty} \mathbf{Pr}(Pattern\ happens\ at\ the\ nth\ trial))^{-1}$$

Reference:

Sheldon Ross. *Stochatic Processes.* Wiley, New York, 1984.

曾经的"数学神童"

陈省身: 1911年生于浙江嘉兴，15岁考入南开大学，21岁在《清华大学理科报告》上发表第一篇学术论文，23岁获硕士学位，25岁获德国汉堡大学博士学位，38岁起担任芝加哥大学的几何学教授，并在十年中复兴了美国的微分几何，形成美国的微分几何学派。

高斯: 1777年生于德国不伦瑞克，有"数学王子"的美誉，和牛顿、阿基米德被誉为有史以来的三大数学家。15岁进入不伦瑞克学院，17岁得到了一个数学史上极重要的结果《正十七边形尺规作图之理论与方法》。

莱布尼兹: 1646出生于德国莱比锡。15岁在莱比锡大学学法律，期间对数学产生浓厚兴趣。20岁发表了第一篇数学论文。从此开始对无穷小算法的研究，独立创立微积分的基本概念与算法，和牛顿共同奠定微积分学。

拉马努金: 1888年出生于印度，二十世纪国际数学界公认的数学奇才，对数论的众多领域作出了开创性贡献。32岁去世，身后留下近4000条未经证明的数学公式和定理，证明它们成为国际数学界的一个重大挑战。

Young men should prove theorems, old men should write books.

—— G. H. Hardy

选择公理的一组等价命题及其意义

07001 申国桢　　刘博睿

摘　要

本文提出并证明了选择公理的一组等价命题，利用它证明了“广义连续统假设蕴含选择公理”，最后对选择公理及其等价命题的意义作了一些讨论.

关键词： 选择公理，良序集，广义连续统假设

§1　问题的提出

我们把所有可以被良序化的集合的全体构成的真类记作 WO.

在ZF形式系统中，任取 $a \in \mathrm{WO}$，a 的幂集 $\mathscr{P}(a)$ 是否一定属于 WO？即“$\mathrm{ZF} \vdash a \in \mathrm{WO} \to \mathscr{P}(a) \in \mathrm{WO}$”是否成立？具体一点，我们知道实数集 $\mathbb{R} \approx \mathscr{P}(\omega)$，在 ZF 中，$\mathbb{R}$ 是不是良序集？

笔者对上述问题进行了一些研究，得出了选择公理的一组等价命题.

§2　选择公理的一组等价命题及其应用

以下证明中将要用到的关于“良基集”的理论见[2]，关于“Hartogs数”的理论见[3]. 证明中将直接使用集合论中关于它们的通用记号.

我们首先作一些简记：

AC:　选择公理

WO:　良序原理：$\forall x(x \in \mathrm{WO})$

AC_1:　$\forall x(x \in \mathrm{WO} \to \mathscr{P}(x) \in \mathrm{WO})$

AC_2:　$\forall x(x \subset \mathrm{WO} \to x \in \mathrm{WO})$

AC_3:　$\forall x(\cup x \in \mathrm{WO} \to x \in \mathrm{WO})$

AC_4: $\forall x, y \in \mathrm{WO}({}^{x}y \in \mathrm{WO})$

首先, [4]中证明了

引理2.1. $\mathrm{ZF} \vdash \mathrm{AC} \leftrightarrow \mathrm{WO}$.

因此, 我们有

引理2.2. $\mathrm{ZF} \vdash \mathrm{AC} \rightarrow (\mathrm{AC}_1 \wedge \mathrm{AC}_2 \wedge \mathrm{AC}_3 \wedge \mathrm{AC}_4)$.

同时, 容易看到

引理2.3. $\mathrm{ZF} \vdash \mathrm{AC}_i \rightarrow \mathrm{AC}_1, i = 2, 3, 4$.

证明. 在ZF中, 若AC_2成立, 设$x \in WO$, 则$\forall y \subset x(y \in \mathrm{WO})$, 故$\mathscr{P}(x) \subset \mathrm{WO}$, 由$\mathrm{AC}_2$, $\mathscr{P}(x) \in \mathrm{WO}$, 即$\mathrm{AC}_1$成立.

若AC_3成立, 设$x \in \mathrm{WO}$, 则$\cup\mathscr{P}(x) = x \in \mathrm{WO}$, 由$\mathrm{AC}_3$, $\mathscr{P}(x) \in \mathrm{WO}$, 即$\mathrm{AC}_1$成立.

若AC_4成立, 设$x \in \mathrm{WO}$, 由AC_4, ${}^{x}2 \in \mathrm{WO}$, 又$\mathscr{P}(x) \approx {}^{x}2$, 故$\mathscr{P}(x) \in \mathrm{WO}$, 即$\mathrm{AC}_1$成立.

所以, 只要能证明$\mathrm{AC}_1 \rightarrow \mathrm{AC}$, 就可以知道$\mathrm{AC}_i(i = 1, 2, 3, 4)$都是AC的等价命题了. □

引理2.4. 在ZF中, 设α为极限序数, $V_\alpha = \cup\{V_\beta | \beta < \alpha\}$, 若有$W = \{W_\beta | \beta < \alpha\}$, 使得$\forall \beta < \alpha$, W_β是V_β上的良序, 则按下式定义的W_α是V_α上的良序:

$$xW_\alpha y \leftrightarrow x, y \in V_\alpha \wedge (\mathrm{rank}x < \mathrm{rank}y \vee (\mathrm{rank}x = \mathrm{rank}y \wedge xW_{\mathrm{rank}(x+1)}y)).$$

证明. 直接验证良序的定义即可. □

下面是本文的主要结果:

定理6. $\mathrm{ZF} \vdash \mathrm{AC}_1 \rightarrow \mathrm{WO}$.

证明. 若AC_1成立, 我们首先证明: $\forall \alpha \in \mathbf{On}(V_\alpha \in \mathrm{WO})$. 对$\alpha \in \mathbf{On}$用超限归纳法:

当$\alpha = 0$时, $V_\alpha = 0 \in \mathrm{WO}$. $\alpha = \beta'$时, 由归纳假设$V_\beta \in \mathrm{WO}$, 由AC_1, $V_\alpha = V_{\beta'} = \mathscr{P}(V_\beta) \in \mathrm{WO}$. α是极限序数时, 由引理4, 只用证明: 存在$W = \{W_\beta | \beta < \alpha\}$, 使得$\forall \beta < \alpha$ (W_β是V_β上的良序), 再对$\beta \in \alpha$进行超限归纳证明W的存在性: $\beta = 0$时, 取$W_\beta = 0$为V_β上的良序. $\beta = \gamma'$时, 由归纳假设, 已有W_γ是V_γ上的良序, 设$\kappa = V_\alpha^+$ (V_α的Hartogs数), 由AC_1, $\mathscr{P}(\kappa) \in \mathrm{WO}$, 取定$R$为$\mathscr{P}(\kappa)$上的良序. 设$(V_\gamma, W_\gamma)$的序型为$\delta$, 由于$V_\gamma < V_\alpha$, 故$\delta < \kappa$, 从而$\mathscr{P}(\delta) \preccurlyeq \mathscr{P}(\kappa)$, 利用$R$又到处$V_\beta$上的良序, 记为$W_\beta$, β为极限序数时, 由归纳假设, 存在$\{W_\gamma | \gamma < \beta\}$, 使得$\forall \gamma < \beta$ (W_γ是V_γ上的良序), 由引理4, 可以定义V_β上的良序W_β. 所以α为极限序数时, $V_\alpha \in \mathrm{WO}$, 所以, $\forall \alpha \in \mathbf{On}(V_\alpha \in \mathrm{WO})$. 那么, 任取$x$, 由于$x \subset V_{\mathrm{rank}\ x}$, 故$x \in \mathrm{WO}$, 即WO成立. □

注: 以上证明并没有使用AC, 在证明$W = \{W_\beta | \beta < \alpha\}$的存在时, 不能用AC直接断言它的存在性, 因为现在的讨论不允许使用AC.

再根据引理1, 就有

定理7. $\mathrm{ZF} \vdash \mathrm{AC}_1 \rightarrow \mathrm{AC}$.

Science is built up of facts, as a house is with stones. But a collection of facts is no more a science than a heap of stones is a house.

—— Henri Poincare

再根据引理2, 3, 就得到了AC的一组等价命题: $\mathrm{AC}_i(i=1,2,3,4)\to\mathrm{AC}$.

将广义连续统假设简记为GCH: $\forall\kappa\in\mathbf{Cn}(\kappa\geqslant\omega\to{}^{\kappa}2\approx\kappa^{+})$

定理8. $\mathrm{ZF}\vdash\mathrm{GCH}\to\mathrm{AC}$.

证明. 若GCH成立, 任取$x\in\mathrm{WO}$, 若$|x|<\omega$, 则显然$\mathscr{P}(x)\in\mathrm{WO}$, 若$|x|\geqslant\omega$, 由GCH, 有$\mathscr{P}(x)\approx{}^{x}2\approx{}^{|x|}2\approx|x|^{+}$, 而$|x|^{+}\in\mathrm{WO}$, 故$\mathscr{P}(x)\in\mathrm{WO}$, 所以, AC_1成立, 由定理2, AC成立. □

§3 意义的讨论

我们将ZF形式系统称之为"形式数学", 而把研究形式数学时用到的数学称之为"元数学"([5]).

ZF6(无限公理)引入后, "实无限"是否合理, 仍是一个未知数, AC的引入正是肯定了元数学中的"实无限"的合理性. (AC相当于允许任意次带有随意性的选取)

从另一个角度来看, AC相当于断言某种个"不可构造的存在"的合理性, 事实上, 从AC的等价命题"Zorn引理", "Hausdorff极大原理", "Tukey引理"等命题中就可以看出.

实际上, 正是AC断言元数学中"实无限"的合理性, 导致了AC相当于断言某种"不可构造的存在"的合理性, 因为"实无限"是人类感官无法真正接触到的, 是"不可构造"的. 这也是"直觉主义"一开始强烈反对AC的主要原因.

有了结论"$\mathrm{AC}\leftrightarrow\mathrm{WO}$"以后, 许多人误认为AC的作用仅仅在于把集类限制在良序集类上, 本文的结果表明: 就连WO自身的一些性质也要依赖于AC!(没有AC, 就没有AC_1, 对于一个$x\in\mathrm{WO}$, 连$\mathscr{P}(x)$是否属于WO都不知道)这也对文初提出的问题给出了否定的回答.

参考文献

[1] 汪芳庭, 数学基础, 北京: 科学出版社, 2001. 144

[2] 汪芳庭, 公理集论, 合肥: 中国科学技术大学出版社, 1995. 44–52

[3] 汪芳庭, 数学基础, 北京: 科学出版社, 2001. 179–181

[4] 张锦文, 公理集合论导引, 北京: 科学出版社, 1991. 174

[5] 汪芳庭, 数理逻辑, 合肥: 中国科学技术大学出版社, 1990. 引言

I realized that anything to do with Fermat's Last Theorem generates too much interest.

—— Andrew Wiles

主编：中国科学技术大学零五级数学系

编委：华淼 涂思铭 王晓辉

汪颖佩 杨馨 杨扬 杨熠

封面设计：韩玮