w domyśle właśnie ε. Zauważmy, że spełnia ono nasze wymaganie (4). Istotnie, baza danych D bez moich danych oraz baza danych D', która powstała przez dodanie do bazy danych D moich danych, różnią się jedynie jednym elementem. Dowolne pytanie na temat bazy danych D, na które odpowiedź jest TAK lub NIE, musi tak naprawdę być postaci: czy nasz raport $\mathcal{A}(D)$ należy do wyróżnionego zbioru raportów $T \subseteq S$. A więc, istotnie, dla każdego pytania prawdopodobieństwo odpowiedzi TAK tylko nieznacznie się zmieni (maksymalnie o około ε) w zależności od tego, czy ja będę uczestniczył w badaniu, czy też nie. Pojęcie prywatności różnicowej unika przykrej własności, którą miała definicja z punktu (3). Mianowicie jeśli zrobimy kilka badań dobrze zachowujących prywatność, to sumarycznie ujawnią one również niewiele prywatności. Łatwo udowodnić, co polecamy Czytelnikowi, że jeśli stworzymy n badań, o prywatności różnicowej odpowiednio $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$, to sumarycznie to badanie będzie miało prywatność różnicową nie większą niż $\sum_{i=1}^{n} \varepsilon_i$. Czyli intuicja mówiąca o tym, że algorytm ε-różnicowo-prywatny „ujawnia ε prywatności", jest dobra – ta miara się sumuje. Oprócz innych zalet tego pojęcia być może najważniejszą jest to, że można stosunkowo łatwo zaprojektować system, który je realizuje. Idea jest bardzo naturalna, po prostu do wyniku zapytania na prawdziwej bazie danych dodaje się losowy szum i dopiero ten zaszumiony wynik się publikuje. Jest wiele różnych mechanizmów realizacji tego pomysłu, bo np. warto inaczej traktować zapytania $\mathcal{A}(D)$ zwracające liczby rzeczywiste, a inaczej takie, które przyjmują tylko skończenie wiele możliwych wartości. Najbardziej znany mechanizm nazywa się mechanizmem Laplace'a i dobrze zachowuje się w sytuacji, gdy $\mathcal{A}(D)$ przyjmuje wartości rzeczywiste z pewnym rozkładem ciągłym. Do wyniku dodaje się w nim zmienną o rozkładzie Laplace'a $\mathrm{Lap}(\lambda)$: jeśli $X \sim \mathrm{Lap}(\lambda)$, to gęstość zmiennej X wyraża się wzorem $g_X(x) = \frac{1}{2\lambda} e^{-\frac{|x|}{\lambda}}$. Zainteresowanego Czytelnika zachęcam do zgłębiania szczegółów. Mimo że pojęcie prywatności różnicowej jest stosunkowo nowe, to w Internecie można o nim znaleźć wiele wartościowych informacji.

Na koniec warto powiedzieć, że pojęcie prywatności różnicowej bardzo szybko zdobywa popularność. Już teraz wielkie firmy technologiczne, takie jak Google, Apple, Microsoft czy Facebook, zaczynają go używać w swoich zastosowaniach. Przykładowo Google stosuje prywatność różnicową przy analizie złośliwego oprogramowania w przeglądarce Chrome i korków w dużych miastach w aplikacji Maps, a Apple przy analizie użycia emotikonów w różnych kontekstach oraz słów niewystępujących w słowniku. Wiele uniwersytetów dodaje do swoich kursów materiały na ten temat. Całkiem prawdopodobne, że jesteśmy w przededniu dużego sukcesu tego pojęcia.

Pół szklanki mocnego kodu

Koniec świata

*Piotr KRZYŻANOWSKI**

* Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

W czasach niepewności, wielkich zmian, kryzysów ludzie więcej myślą o sprawach ostatecznych. *Czy to nie zbliża się koniec cywilizacji, a może nawet całego świata?* W dawnych czasach dobrym wzorem ładu i uporządkowania był Kosmos w dostatecznie dużej skali. No bo przecież nie Ziemia, ze swoją przyziemną nieprzewidywalnością – ale już jej wspólna podróż z Księżycem wokół Słońca, od „zawsze" taka sama, mogłaby stanowić jakiś punkt odniesienia. Albo jeszcze lepiej: popatrzmy na cały Układ Słoneczny! Czy jego leniwie przemierzające przestrzeń planety są oazą spokoju, przewidywalności i stabilności – jeśli nie na *wieczność*, to może przynajmniej na miliony, lub lepiej miliardy, lat? Jak trudno rozstrzygnąć to pytanie na gruncie matematyki, przekonał się sam wielki Henri Poincaré. Ale od czego są komputery... zwłaszcza że praktycznie sprawa jest bardzo prosta: należy zbadać trajektorie ruchu planet w interesującym nas okresie. Skoro planety poruszają się w próżni, na ich ruch ma wpływ jedynie siła grawitacji ze strony pozostałych ciał: przede wszystkim Słońca, którego masa jest około milion razy większa od łącznej masy wszystkich planet.

Pod koniec XIX wieku król Szwecji i Norwegii ogłosił z okazji urodzin konkurs na rozwiązanie zagadnienia ruchu planet. Konkurs wygrał 35-letni Henri Poincaré. Jednak w jego pracy, którą w międzyczasie opublikowano, tkwił poważny błąd. Gdy się zorientował, wykupił cały jej nakład – co kosztowało go więcej niż królewska nagroda. Za to poprawiona wersja artykułu położyła podwaliny teorii chaosu.

W najprostszej sytuacji – gdy jest tylko Słońce, o masie m_1, i jedna planeta, o masie m_2, – przyciągają się one z siłą grawitacji o wartości

$$F = G\frac{m_1 \cdot m_2}{r^2},$$

działającą wzdłuż łączącego je promienia długości r. W ogólnym przypadku, gdy mamy do czynienia z **zagadnieniem N ciał**, jest analogicznie: wypadkowa siła działająca na i-te ciało będzie sumą sił przyciągania go przez pozostałe.

W naszym przypadku $N = 10$: Słońce plus osiem planet (w tym Ziemia) i, z sentymentu, Pluton.

Ponieważ, jak pamiętamy z lekcji fizyki, przyspieszenie jest proporcjonalne do siły, $\vec{F} = m \cdot \vec{a}$, a przecież przyspieszenie $\vec{a} = \dfrac{\Delta\vec{v}}{\Delta t}$ i podobnie $\vec{v} = \dfrac{\Delta\vec{x}}{\Delta t}$, to mnożąc te równości przez Δt dostajemy układ równań

$$\begin{cases} \Delta\vec{x}_i = \Delta t \cdot \vec{v}_i, \\ \Delta\vec{v}_i = \Delta t \cdot \sum_{j\neq i} \vec{F}_{ij}/m_i, \end{cases} \qquad \text{dla } i = 1, \ldots, N.$$

Ponieważ $\Delta\vec{x} = \vec{x}^{\,\text{nowe}} - \vec{x}^{\,\text{stare}}$ i podobnie $\Delta\vec{v} = \vec{v}^{\,\text{nowe}} - \vec{v}^{\,\text{stare}}$, a siła przyciągania $\vec{F}_{ij}$ pomiędzy ciałem i-tym a j-tym zależy właśnie od $\vec{x}_i$ i $\vec{x}_j$, to powyższe jest zamkniętym układem $2N$ równań (wektorowych w przestrzeni trójwymiarowej), które wystarczy rozwiązać, na przykład takim oto algorytmem:

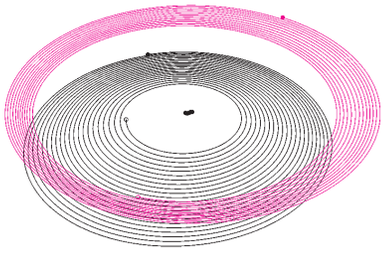
$$\begin{cases} \vec{x}_i{}^{\,\text{nowe}} = \vec{x}_i{}^{\,\text{stare}} + \Delta t \cdot \vec{v}_i{}^{\,\text{stare}}, \\ \vec{v}_i{}^{\,\text{nowe}} = \vec{v}_i{}^{\,\text{stare}} + \Delta t \cdot \sum_{j\neq i} \vec{F}_{ij}{}^{\,\text{stare}}/m_i. \end{cases}$$

Rzeczywiście, znając *stare* wartości prędkości i położenia wszystkich ciał, możemy na ich podstawie wyznaczyć z powyższego wartości *nowe*, tzn. po czasie Δt. Okazuje się, że wyprowadzona przez nas metoda to nic innego, jak znany i popularny schemat Eulera. O tym, że wspaniale radzi sobie np. w modelowaniu chorób zakaźnych, można było przeczytać w *Delcie* 5/2018.

Naszym celem będzie teraz zbadanie, czy Układ Słoneczny nie rozpadnie się przez, powiedzmy, najbliższe 10 tysięcy lat – w ludzkiej skali to dostatecznie długi czas. Masy oraz dzisiejsze początkowe położenia i prędkości wszystkich obiektów pobierzemy ze strony internetowej NASA, dotyczącej projektu Horizons. Przy tak długim czasie symulacji użyjemy niesamowicie krótkiego kroku czasowego, $\Delta t = 2$ godz., i bardzo szybkiego komputera. Fani rubryki o *mocnym* kodzie wybaczą mi, że jedynie w *pseudokodzie* naszkicuję sedno powyższego algorytmu (prawdziwą implementację, z której pochodzą obrazki, zrobiłem w MATLAB-ie):

Schemat Eulera:

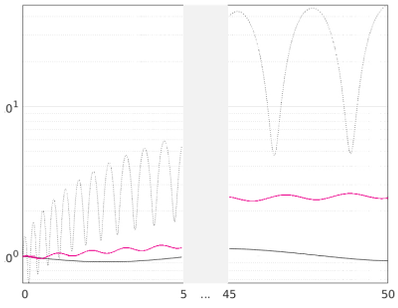
```
t = 0; T = 500 lat; dt = 2 godziny;
x = (*..położenia początkowe..*); v = (*..prędkości początkowe..*);
while t < T
  F = siła_wypadkowa(x);
  x = x + dt*v;
  v = v + dt*F;
  t = t + dt;
end
```



Orbity Ziemi (pomarańczowa) i Merkurego przez najbliższe 15 lat. Obie planety oddalają się od Słońca, a na koniec Merkury jest nawet dalej niż Ziemia!

Co wynika z przeprowadzonych symulacji? **Wieści są nad wyraz niepokojące**. Z wykresu obok wynika, że jeszcze w obecnym stuleciu Merkury zostanie wytrącony ze swojej orbity!

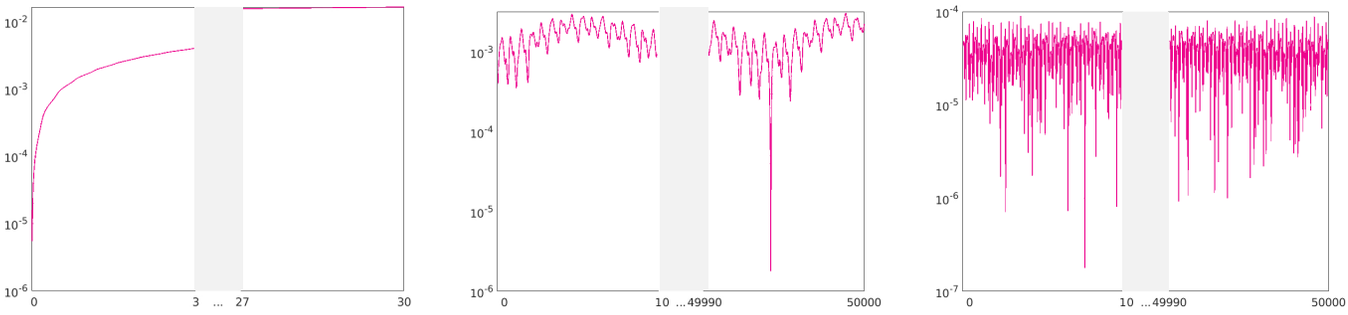
Co gorsza, symulacja przewiduje, że podobny los czeka Wenus i Ziemię: zaledwie za 30 lat promień naszej orbity wzrośnie dwa razy – co spowoduje, że będzie do nas docierać 8 razy mniej energii ze Słońca. Nic nie pomoże, nawet globalne ocieplenie: nasza planeta zacznie zamarzać. Za mniej niż 500 lat Ziemia znajdzie się 10 razy dalej od Słońca, a to już oznacza całkowity i nieodwołalny koniec... Tylko odległe planety–olbrzymy: Jowisz, Saturn, Uran i Neptun przetrwają ten kataklizm.



Wycinek zmian odległości od Słońca względem odległości początkowej przez najbliższe 50 lat: Merkury – linia kropkowana, Ziemia – pomarańczowa, Jowisz – czarna. Tylko Jowisz nie opuszcza orbity

Czy to prawda? Czy rzeczywiście jeszcze za naszego życia czekają nas tak dramatyczne wydarzenia? Dlaczego tak musi się stać? Przyjrzyjmy się otrzymanym rozwiązaniom raz jeszcze, ale z innej strony – i zastanówmy się, czy czasem nie **zostaliśmy oszukani**. Na wykresach na następnej stronie możemy zobaczyć, jak bardzo wraz z upływem czasu całkowita energia układu odchyla się od wartości początkowej.

Okazuje się, że schemat Eulera, który przecież tak dobrze sprawdza się w wielu innych sytuacjach, tutaj napotyka poważny problem: w sposób sztuczny *pompuje do układu energię*, której już po kilkudziesięciu latach przybywa kilka procent! Jasne więc, że wiele ciał tego nie wytrzymuje i urywa się z orbit – tyle, że



Względna zmiana energii całkowitej układu w czasie. Od lewej: schemat Eulera (1% już po 50 latach), symplektyczny schemat Eulera (10^{-3} przez 50 tysięcy lat), schemat Verleta (10^{-4} przez 50 tysięcy lat)

jest to wyłącznie artefakt symulacji: w końcu prawdziwe planety zasada zachowania energii przecież obowiązuje. Problem nierespektowania fizycznych zasad zachowania dotyczy nie tylko schematu Eulera, ale też wielu innych popularnych metod numerycznych wyznaczania trajektorii układów dynamicznych. Na przykład znana i lubiana metoda RK4, dużo dokładniejsza od Eulera, też cierpi na podobną chorobę: w niej z kolei energia powoli, ale nieubłaganie... znika.

Z drugiej strony, zgodnie z teorią zbieżności schematu Eulera, wystarczy *dostatecznie* zmniejszyć Δt, by z *dowolną* zadaną dokładnością uzyskać rozwiązanie. Jednak w moim przypadku zmniejszenie Δt do minut lub – być może – sekund nie wchodzi w grę z prozaicznych powodów: nie mam *aż tak* szybkiego komputera!

Jest jednak promyk nadziei: można **ulepszyć** schemat Eulera **jednym** subtelnym ruchem ręki – i nie jest to gest sięgania po kartę kredytową w celu kupna nowego komputera. Wystarczy po prostu *zmienić kolejność dwóch instrukcji* w pętli, o tak:

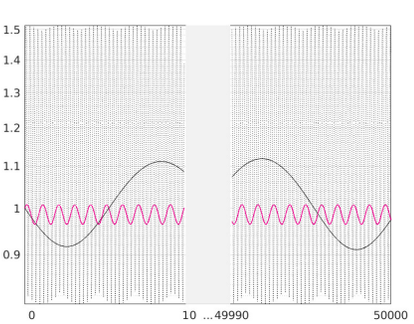
Ten schemat odkryła Abby Aspel. Sprawdzając, czy nie pomyliła się w programowaniu metody Eulera, zmieniła kolejność instrukcji w pętli!

Symplektyczny schemat Eulera:

```
t = 0; T = 500 lat; dt = 2 godziny;
x = (*..położenia początkowe..*); v = (*..prędkości początkowe..*);
while t < T
  F = siła_wypadkowa(x);
  v = v + dt*F;
  x = x + dt*v;
  t = t + dt;
end
```

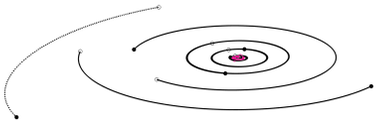
Jak widać na środkowym wykresie na górze strony, tym razem energia nie jest co prawda idealnie zachowana, ale przynajmniej oscyluje wokół pierwotnej wartości. Orbity uzyskane w ten sposób przez tysiące lat trzymają fason i nie rozwijają się w dramatyczne spirale. Jeszcze lepsza – i jednocześnie dokładniejsza – jest metoda *leap–frog*, zwana też schematem Verleta.

Wykres obok pokazuje, że w jej przypadku odchylenie nie przekroczyło jednej dziesięciotysięcznej na przestrzeni 50 tysięcy lat!



Wycinek zmian odległości od Słońca względem odległości początkowej przez najbliższe **50 tysięcy** lat, obliczony schematem Verleta z $\Delta t = 10$ dni. Merkury – linia kropkowana, Ziemia – pomarańczowa, Jowisz – czarna. Tym razem wszystko przebiega cyklicznie, jak w zegarku

I tym sposobem, po zmianie schematu na symplektyczny schemat Eulera (a tym bardziej na metodę *leap–frog*), **Świat został uratowany**: przez kolejne dziesiątki tysięcy lat – jak na rysunku obok – ruch planet jest uspokajająco cykliczny, jak w zegarku. Układ Słoneczny trzyma się stabilnie!



Trajektorie wszystkich planet przez końcowe 70 lat z symulacji schematem Verleta obejmującej **50 tysięcy** lat. Kropkowaną linią zaznaczono orbitę Plutona (która i teraz jest aż tak ekscentryczna). Pomarańczowa kropka w środku to orbita Ziemi

Może więc nie będzie tak źle?