przesunięcia) prowadzi do zasady zachowania pędu, i *vice versa*. Podobny związek zachodzi między składowymi wektora momentu pędu czy też energią a czasem. Stąd można się spodziewać, że istnieje wiele zasad nieoznaczoności, łączących rozrzuty pomiarów dwóch *sprzężonych* wielkości fizycznych.

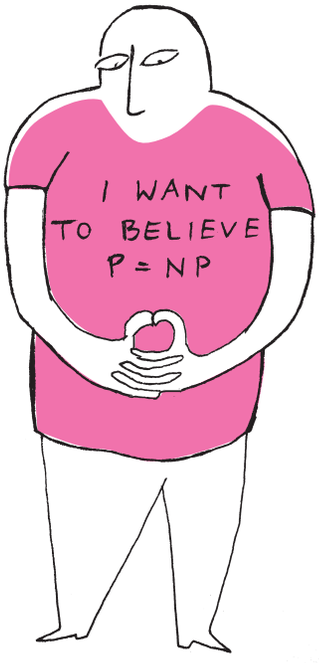
Poza żywymi i martwymi kotami czy wysoce hipotetycznymi komputerami kwantowymi to zasada nieoznaczoności jest jednym z tych pojęć powstałych na gruncie teorii kwantów, które zdołały się przebić do powszechnej świadomości. Zazwyczaj formułowana jest w sposób niemający wiele wspólnego z powyższym wyprowadzeniem: powiada się, że pomiar położenia tak zaburza układ, że następujący po nim pomiar pędu daje wyniki z dużym rozrzutem, i na odwrót. Zauważmy, że w naszym opisie pomiary nie są wykonywane sekwencyjnie na jednej cząstce, lecz na wielu kopiach tego samego stanu kwantowego. Lecz bez względu na sformułowanie zasada nieoznaczoności Heisenberga pozostaje jedną ze zdumiewających konsekwencji kwantowej superpozycji.

Ludziom małej wiary

Tomasz KAZANA

Świat informatyki teoretycznej pełen jest hipotez, które badacze przyjmują po prostu *na wiarę*. Niektórzy wierzą, na przykład, że P $\neq$ NP, inni wierzą, że istnieje bezpieczna kryptografia klucza publicznego (albo jeszcze konkretniej: wierzą, że szyfrowanie RSA jest bezpieczne). Co ciekawe, najpopularniejsze hipotezy informatyczne bynajmniej nie są równoważne, a relacje między nimi mogą zaskakiwać.

Chyba najpiękniej tę tematykę omówił Russell Impagliazzo w swym popularnym artykule *A Personal View of Average-Case Complexity* z roku 1995. Znajdziemy tam omówienie pięciu potencjalnych Wszechświatów, w których różne hipotezy mają różne rozstrzygnięcia. Scharakteryzujmy pokrótce te miejsca.



Wszechświat *Algorithmica.* Tutaj zakładamy, że po prostu P = NP. Filozoficznie oznacza to, że w zasadzie nie ma dla nas problemów bardzo trudnych. Niemal wszystkie problemy obliczeniowe komputer potrafi rozwiązywać w czasie wielomianowym.

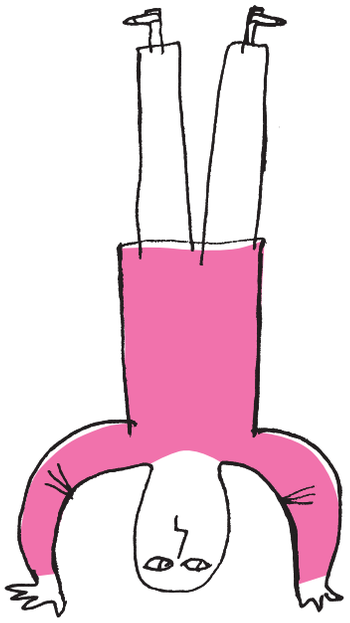
Wszechświat *Heuristica.* Tym razem co prawda P $\neq$ NP, ale generalnie tragedii obliczeniowej nie ma. Impagliazzo rozumie to w ten sposób, że istnieją problemy z klasy NP, dla których nie ma algorytmów, które *zawsze* działają w czasie wielomianowym, jednakże dla każdego takiego problemu istnieje algorytm, który dla przeciętnej jego instancji działa już szybko. Co więcej: te trudne instancje problemów NP są również trudne do znalezienia, a więc i tak nie powinny się pojawić w praktyce.

Wszechświat *Pessiland.* Tutaj istnieją problemy z klasy NP, które są trudne również w średnim przypadku. Dodatkowo nie istnieją funkcje jednokierunkowe (szerzej o nich niżej).

Wszechświat *Minicrypt.* W tym miejscu istnieją funkcje jednokierunkowe, a więc takie, których wartości komputer może szybko obliczać, ale dla których problem szukania przeciwobrazu jest trudny. Funkcje jednokierunkowe odgrywają dużą rolę w kryptologii. Z drugiej jednak strony zakładamy, że w Minicrypcie nie istnieje bezpieczna kryptografia klucza publicznego.

Wszechświat *Cryptomania.* W tych okolicach występują i funkcje jednokierunkowe, i bezpieczna kryptografia klucza publicznego.

To, w którym z powyższych Wszechświatów my żyjemy, jest dzisiaj kwestią wiary. Pierwsze dwa światy to, oczywiście, eldorado algorytmików. Zarówno w Algorithmice, jak i w Heuristice niemal nie ma praktycznych problemów, dla których wielomianowa maszyna Turinga byłaby bezużyteczna. Z drugiej strony Minicrypt i Cryptomania to krainy mlekiem i miodem płynące dla kryptologów. Tylko tam istnieją jakiekolwiek nietrywialne protokoły kryptologiczne.



Najsmutniejszym miejscem dla wszystkich (Mordorem informatyków?) zdaje się być (nienazwany przecież przypadkowo) Pessiland. Brakuje w nim funkcji jednokierunkowych, więc kryptolodzy są bezrobotni. Z drugiej strony algorytmicy też są bezsilni wobec wielu problemów z klasy NP.

W kwestii publicznych wyznań wiary to w znakomitej większości informatycy wierzą, że żyjemy w Cryptomanii. W większości, ale z całą pewnością nie jednomyślnie. Bardzo poważną i bardzo szanowaną osobą, która skłania się ku wierze w Algorithmikę, jest podobno profesor Wojciech Rytter z Uniwersytetu Warszawskiego. Autor niniejszego tekstu nie miał śmiałości, aby ten fakt zweryfikować u źródła. Ten sam autor ma również opory, żeby w druku pojawiła się jego osobista opinia w rozważanym temacie. Zresztą, jak w tym dowcipie o góralu, co to wstąpił do PZPR, i tak się z nią nie zgadza.

Jak już wspomniano na wstępie, dość interesujące są niektóre implikacje. Na przykład umiemy udowodnić, że jeśli funkcje jednokierunkowe istnieją, to musi być $\mathrm{P} \neq \mathrm{NP}$. (Rozumowanie jest w zasadzie natychmiastowe: gdyby $\mathrm{P} = \mathrm{NP}$, to odwracanie jakiejkolwiek funkcji nie mogłoby być istotnie trudniejsze od jej obliczania, bo przecież szukanie przeciwobrazu to problem z klasy NP; ta ostatnia obserwacja jest natychmiastowa, gdyż sam przeciwobraz może posłużyć jako *świadek* z definicji klasy NP.)

Z drugiej strony nie jest jasne, czy z założenia $\mathrm{P} \neq \mathrm{NP}$ wynika istnienie funkcji jednokierunkowych. Jest to bardzo ważny otwarty problem informatyki teoretycznej. Gdyby został pozytywnie rozstrzygnięty, przynajmniej przestałaby nas nękać apokaliptyczna wizja Pessilandu.

Na moment wróćmy jeszcze do Minicryptu. Ładną własnością tego Wszechświata jest mnogość jego równoważnych definicji. Otóż okazuje się, że istnienie funkcji jednokierunkowych jest równoważne każdej z następujących hipotez.

- Istnieje generator pseudolosowy. To znaczy: istnieje funkcja (łatwo obliczalna) $f : \{0,1\}^n \to \{0,1\}^m$, gdzie $m > n$ oraz taka, że (dla wielomianowej maszyny Turinga) jednostajnie wylosowany element z $\{0,1\}^m$ jest nieodróżnialny od $f(U)$, gdzie U wylosowano również jednostajnie, ale z mniejszego zbioru $\{0,1\}^n$.
- Istnieje permutacja pseudolosowa oraz funkcja pseudolosowa.
- Istnieje bezpieczne szyfrowanie symetryczne z kluczami krótszymi od wysyłanych wiadomości.
- Istnieją ukochane (jakieś osobiste wyznanie wiary jednak się tu znajdzie) przez autora niniejszego tekstu protokoły z wiedzą zerową (Zero-Knowledge Proofs).
- Istnieje bezpieczny podpis cyfrowy.

Jako się rzekło, wszystkie powyższe zdania są równoważne. Jednak, oczywiście, nie każda implikacja jest jednakowo interesująca. Niektóre z nich można potraktować jako ćwiczenia dla Czytelnika (np. jak z generatora pseudolosowego *zrobić* szyfrowanie symetryczne, a następnie: jak z szyfrowania *zrobić* funkcję jednokierunkową). Inne – były wyzwaniem dla badaczy tej dziedziny. Szczególnie ciekawa jest implikacja

$$\textit{funkcja jednokierunkowa} \implies \textit{generator pseudolosowy},$$

czyli tak zwane twierdzenie HILL (od nazwisk Hastad, Impagliazzo, Levin, Luby).

Jak nietrudno zauważyć, powyższa lista równoważnych hipotez obejmuje niemal całą kryptologię. Niemal, bo nie zawiera kryptografii klucza publicznego. Jest to o tyle dziwne, że zawiera podpis cyfrowy, który *na oko* jest problemem podobnej klasy. A jednak! Nikt nie udowodnił jeszcze, że za pomocą funkcji jednokierunkowej potrafimy *zrobić* szyfrowanie asymetryczne. Gdyby było inaczej, okazałoby się, że definicja Impagliazzo Minicryptu jest wewnętrznie sprzeczna, a kryptolodzy powinni (co i tak zwykle robią) celować w Cryptomanię...

Ustalenie, który z opisanych wyżej Wszechświatów jest tym naszym, jest, być może, największym wyzwaniem informatyki w XXI wieku. Kto wie, w jakim Wszechświecie obudzimy się za kilka, kilkanaście lat...

Wbrew obiegowej opinii nie umiemy wykazać, że bezpieczeństwo kryptosystemu klucza publicznego RSA daje się zredukować do problemu trudności rozkładu na czynniki pierwsze. Zresztą trudność rozkładu jest również tylko hipotetyczna. Oba te poglądy stanowią jedne z prawd wiary kryptologów.