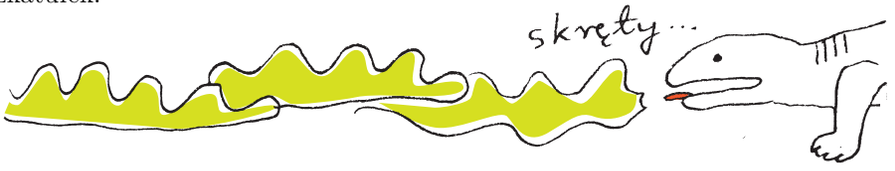
odszyfrowany kluczem a przez Artura. Wtedy te trzy przesyłane teksty to kolejno $t \oplus a$, $t \oplus a \oplus b$ oraz $t \oplus a \oplus b \oplus a = t \oplus b$.

Sksorowanie tych trzech zaszyfrowanych wiadomości to $(t \oplus a) \oplus (t \oplus a \oplus b) \oplus (t \oplus b)$, co z uwagi na łączność i przemienność funkcji xor daje nam $(t \oplus t) \oplus (a \oplus a) \oplus (b \oplus b) \oplus t = 0 \oplus 0 \oplus 0 \oplus t = t$. Bez żadnego wysiłku z tych trzech tekstów odtworzymy zaszyfrowaną wiadomość t.

Klasycznym rozwiązaniem naszego problemu w kryptografii jest *protokół Diffiego–Hellmana* pozwalający ustalić stronom komunikacji *wspólny* klucz szyfrowania w bezpieczny sposób.

Zauważmy, jak ważne w kryptografii jest wyspecyfikowanie celu – tu jest nim niemożliwość lub wystarczająca trudność odtworzenia zaszyfrowanego tekstu przez podglądacza bez znajomości kluczy szyfrujących. Tej istotnej własności niestety naszej metodzie brakuje.

A najciekawsze jest to, że algorytm Artura z fizycznymi kłódkami działa i jest nie do złamania, nawet jeśli kurier przez jakiś czas ma dostęp do zamkniętych szkatułek.



Do powierzchni obrotowych i jeszcze dalej

*Michał MIŚKIEWICZ**

* Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Full ahead, mr. Sulu, maximum warp.

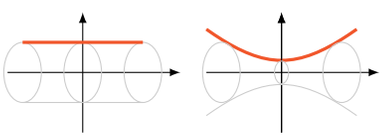
James T. Kirk,
Star Trek: The Original Series, S01E08

Bohaterem tego artykułu jest *produkt skręcony*, po angielsku: *warped product*. Słowo *warp* (wykrzywić, odkształcić) zrobiło karierę za sprawą *warp drive*, hipotetycznego napędu pozwalającego rozwijać prędkości nadświetlne. Został on spopularyzowany w serii science fiction Star Trek i doczekał się całkiem poważnego traktowania, o czym więcej można przeczytać w *Opowieściach o podróżach w kosmos* z Δ^5_{13}, lub też wyszukując hasło *Alcubierre drive*. Wpływ tej idei na zbiorową wyobraźnię jest na tyle duży, że w 2020 roku amerykańska inicjatywa rozwoju i dystrybucji szczepionek przeciwko covid-19 przyjęła nazwę *Operation Warp Speed*.

Oficjalne logo *Operation Warp Speed*, partnerstwa publiczno-prywatnego mającego na celu szybki rozwój i dystrybucję szczepionek przeciwko covid-19 (maj 2020 – luty 2021).

Nazwa nie jest jedyną cechą łączącą produkt skręcony z napędem warp. Po pierwsze, napęd ten opiera się na pomyśle odkształcania przestrzeni, co rodzi pojęciową trudność: wszak umiemy giąć dwuwymiarową kartkę w trójwymiarowej przestrzeni, ale jak mielibyśmy wyginać samą przestrzeń? Odpowiedzią na tę trudność jest geometria wewnętrzna, czyli język pozwalający opisywać geometrię i deformacje obiektu samego w sobie, bez odwołań do otaczającej go przestrzeni. Produkt skręcony jest właśnie jednym z narzędzi takiego opisu.

Po drugie, przekroczenie prędkości światła konwencjonalnymi metodami nie jest możliwe. Furtkę do obejścia tego zakazu proponuje napęd warp. Ograniczenie „prędkości” podobnej natury zobaczymy niżej, badając bliżej powierzchnie obrotowe. Przekonamy się, że produkt skręcony umożliwia pokonanie tej granicy. Zachęcam więc Czytelnika do lektury, by *odkrywać dziwne nowe światy* oraz *śmiało pójść tam, gdzie żaden człowiek wcześniej nie dotarł*.

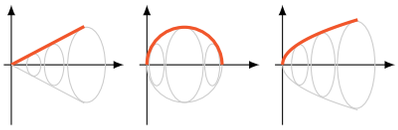


Rys. 1. Walec ($f = \text{const.}$) i hiperboloida jednopowłokowa ($f(x) = \sqrt{1+x^2}$) jako powierzchnie obrotowe. Katenoida ($f(x) = \cosh(x) = \frac{e^x+e^{-x}}{2}$) wygląda podobnie do hiperboloidy

Powierzchnie obrotowe. Przepis na taką powierzchnię jest prosty. Bierzemy ciągłą dodatnią funkcję $f\colon \mathbb{R} \to (0,\infty)$ i jej wykres $y = f(x)$ obracamy wokół osi x. Otrzymaną powierzchnię można opisać równaniem $r = f(x)$, jeśli przez $r = \sqrt{y^2+z^2}$ oznaczymy odległość od osi x.

Przykłady można mnożyć. Przyjęcie za f funkcji stałej prowadzi do konstrukcji walca. Obrót hiperboli, czyli wykresu funkcji $f(x) = \sqrt{1+x^2}$, prowadzi do hiperboloidy jednopowłokowej. Powierzchnię tę zobaczymy też, obserwując szybko obracającą się kostkę (jak na początku filmu [M]). Z kolei funkcja

[M] Mathologer, *Why don't they teach simple visual logarithms (and hyperbolic trig)?*, film na platformie YouTube: youtu.be/G0Fa5Zl-Z3c.



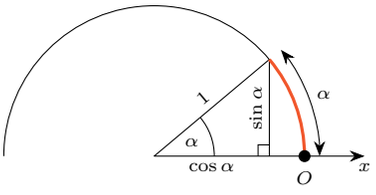
Rys. 2. Stożek, sfera i paraboloida eliptyczna. W każdym z tych przypadków mamy $f(0) = 0$, co oznacza, że powierzchnia się „zamyka” – jak widać, da się to nawet zrobić gładko

$f(x) = \frac{e^x+e^{-x}}{2}$, zwana cosinusem hiperbolicznym, daje nam powierzchnię znaną jako katenoida, która wyróżnia się swoją *minimalnością* (więcej w Δ_{96}^{10}).

Oczywiście funkcja f może mieć mniejszą dziedzinę, wówczas otrzymana powierzchnia ma brzeg w kształcie jednego lub więcej okręgów. Można też dopuścić, by f przyjmowała w jakimś punkcie wartość 0, co w efekcie „zamyka” powierzchnię. Najprostszym przykładem będzie tu stożek, czyli kształt czapeczki urodzinowej. Otrzymujemy ją, wycinając z (nieskończonej) kartki papieru kąt o rozwartości $\alpha \in (0, 2\pi)$ i odpowiednio zginając. Efektem jest powierzchnia opisana przez $f(x) = cx$ dla $x \geqslant 0$, o ile odpowiednio dobierzemy c; musi ono spełniać $\frac{\alpha}{2\pi} = \frac{c}{\sqrt{1+c^2}}$.

Stożek posiada charakterystyczny punkt, wierzchołek, w którym jest niegładki. Można tego uniknąć – wystarczy zażądać, by w punkcie „zamknięcia” pochodna f była nieskończona. Przykład? Sfera jednostkowa jest zadana równaniem $x^2 + y^2 + z^2 = 1$, co możemy przepisać jako $r^2 = 1 - x^2$, a więc powierzchnia ta powstaje z obrotu wykresu $f(x) = \sqrt{1-x^2}$ ($x \in [-1, 1]$). Innym przykładem jest paraboloida eliptyczna, zadana równaniem $x = y^2 + z^2$, a więc pochodząca od funkcji $f(x) = \sqrt{x}$ ($x \geqslant 0$).

Opis wewnętrzny. Dotychczasowy opis można podsumować tak: mierzymy odległość wzdłuż osi x, a dla wybranej wartości x_0 funkcja f mówi nam, jak duży jest okrąg „w odległości x_0”; bardziej ściśle, okrąg stanowiący przekrój płaszczyzną $x = x_0$ ma promień $f(x_0)$. Zamiast wzdłuż osi x moglibyśmy jednak mierzyć odległości wzdłuż samej powierzchni, czyli wzdłuż krzywych powstałych przez obrót wykresu f – jest to sposób bardziej *wewnętrzny*, mający więcej wspólnego z geometrią samej powierzchni. Najłatwiej jest to wyrazić dla powierzchni obrotowej posiadającej punkt $O = (x_0, 0, 0)$ na osi x, czyli dla funkcji f zerującej się w x_0. Przyjmiemy mianowicie, że $h(s)$ jest promieniem okręgu złożonego z punktów odległych od O o s.



Rys. 3. Jeśli odległość od punktu $O = (1, 0, 0)$ liczymy wzdłuż samej sfery, to punkty odległe o α tworzą okrąg o promieniu $\sin\alpha$

Dla pełnej jasności wróćmy do przykładu sfery, w którym jako punkt O możemy przyjąć $(1, 0, 0)$. Punkty odległe od O o α leżą w przekroju $x = \cos\alpha$ i tworzą okrąg o promieniu $\sin\alpha$, a więc $h(\alpha) = \sin\alpha$. Warto zaznaczyć, że odległość liczymy tutaj po najkrótszej krzywej leżącej na sferze, a więc po łuku koła wielkiego, a nie po odcinku – inaczej odległość ta wynosiłaby $2\sin\frac{\alpha}{2}$. Dla porównania dwóch podanych tu sposobów opisu umieśćmy dotychczasowe przykłady w jednej tabelce.

Gdy rozważana powierzchnia obrotowa nie dotyka osi x, należy wybrać jakiś przekrój $x = x_0$ i odległość s liczyć od niego – z plusem w jedną stronę i z minusem w drugą.

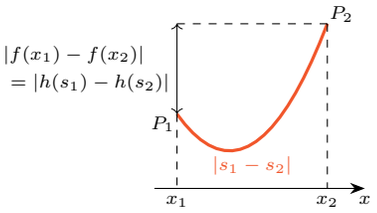
Powierzchnia	Funkcja $f(x)$	Funkcja $h(s)$
Walec o promieniu R	R	R
Katenoida	$(e^x + e^{-x})/2$	$\sqrt{1+s^2}$
Stożek zadany kątem α	cx $(\frac{\alpha}{2\pi} = \frac{c}{\sqrt{1+c^2}})$	$\frac{\alpha}{2\pi}s$
Płaszczyzna		s
Sfera o promieniu R	$\sqrt{R^2 - x^2}$	$R \cdot \sin\frac{s}{R}$
Warunek „gładkiego zamknięcia”:	$f'(x_0) = \pm\infty$	$h'(s_0) = \pm 1$

Zaawansowanych Czytelników może zainteresować, że w literaturze produkt skręcony definiuje się ściśle przy użyciu pojęcia metryki Riemanna. W przypadku sfery byłaby to metryka

$$g(s,\theta) = \underbrace{ds^2}_{\text{m. na odcinku}} + (\sin s)^2 \underbrace{d\theta^2}_{\text{m. na okręgu}}$$

dla $s \in [-1, 1]$ i θ na okręgu, przy czym symbole ds^2 i $d\theta^2$ odnoszą się do standardowej metryki Riemanna na odcinku i okręgu jednostkowym. W pozostałych przypadkach jest podobnie, tylko funkcję sinus należy zastąpić przez odpowiednią funkcję h, a odcinek ewentualnie podmienić na półprostą – w ten sposób opisujemy wszystkie powierzchnie posiadające symetrię obrotową.

W ten sposób poznaliśmy właśnie, czym jest *produkt skręcony* półprostej (lub odcinka) z okręgiem. Żeby ten sposób opisu całkowicie oderwać od otaczającej przestrzeni trójwymiarowej, odnotujmy pewien prosty fakt. Otóż zamiast mówić, że punkty w odległości s od O tworzą w przestrzeni trójwymiarowej okrąg o promieniu $h(s)$, możemy powiedzieć, że tworzą one krzywą (konkretnie okrąg) o długości $2\pi h(s)$. W tym sformułowaniu przestaje mieć znaczenie, jak nasza powierzchnia się układa w przestrzeni – dla przykładu, gdybyśmy czapeczkę urodzinową z powrotem rozłożyli na płasko, to dalej możemy zmierzyć długość krzywej tworzonej przez punkty odległe od wierzchołka o s (tym razem będzie to łuk okręgu, ale nadal o długości αs). O pożytku płynącym z pojęcia skręconego produktu niech świadczy fakt, że można przy jego użyciu opisać metrykę Schwarzschilda, która w ogólnej teorii względności zadaje pole grawitacyjne na zewnątrz sferycznej masy.



Rys. 4. Odległość dwóch punktów, P_1, P_2, liczona wzdłuż wykresu $|s_1 - s_2|$ jest co najmniej taka, jak ich odległość w pionie $|h(s_1) - h(s_2)|$

Uwaga, ograniczenie! Po bliższym przyjrzeniu się tabelce widzimy, że o ile za f można przyjąć dowolną dodatnią funkcję, to już za h niekoniecznie. Każda z podanych wyżej funkcji h ma pochodną ograniczoną w module przez 1 lub innymi słowy: spełnia warunek Lipschitza $|h(s_1) - h(s_2)| \leqslant |s_1 - s_2|$ dla dowolnych s_1, s_2. Dowód, że *tak być musi*, nie jest trudny. Przyjmijmy, że na wykresie funkcji f dany jest punkt $P_1 = (x_1, f(x_1))$ odległy od O o s_1 oraz podobnie opisany punkt P_2 (rys. 4). Ich odległość wzdłuż wykresu wynosi $|s_1 - s_2|$, jednocześnie można ją ograniczyć z dołu przez odległość wzdłuż osi pionowej, czyli $|f(x_1) - f(x_2)|$. Ta ostatnia wielkość to nic innego jak $|h(s_1) - h(s_2)|$, uzasadniliśmy więc warunek Lipschitza.

Czy zatem jesteśmy skazani na rozważanie wyłącznie wolno rosnących funkcji h? Oczywiście, że nie! Dzięki temu, że produkt skręcony posiada interpretację niezależną od otaczającej przestrzeni, możemy nadać geometryczny sens również powierzchniom zadanym abstrakcyjnie przez szybko rosnące funkcje. Narzuca się na przykład rozważenie uogólnienia stożka: funkcja $h(s) = \frac{\alpha}{2\pi} s$ dla $\alpha \geqslant 2\pi$. Przypadek $\alpha = 2\pi$ jest graniczny, odpowiada po prostu płaszczyźnie. Dla $\alpha > 2\pi$ warto samodzielnie wykonać następujący eksperyment: rozcinamy kartkę papieru wzdłuż półprostej, doklejamy brakujący fragment, by otrzymać kąt o rozwartości α, a następnie odpowiednio zginamy. Jak łatwo się przekonać, w przestrzeni „brakuje miejsca", by powstał stożek o symetrii obrotowej. Nie zmienia to faktu, że powierzchnia ta posiada symetrię obrotową w bardziej abstrakcyjnym, wewnętrznym sensie. Pewien niedosyt może oczywiście powodować osobliwość wierzchołka takiego „stożka", dlatego na koniec rozważymy inny, bardzo klasyczny przykład.

Strange new worlds. Za funkcję h przyjmijmy teraz sinus hiperboliczny, czyli funkcję $\sinh(s) := \frac{e^s - e^{-s}}{2}$. Jej pochodną jest wspomniany wcześniej cosinus hiperboliczny $\frac{e^s + e^{-s}}{2}$, który poza $s = 0$ przyjmuje wartości większe od jedynki, co wynika z nierówności między średnią arytmetyczną a geometryczną. Mamy więc do czynienia z egzotyczną powierzchnią zwaną *płaszczyzną hiperboliczną*, która podobnie jak stożek nie daje się zrealizować jako powierzchnia obrotowa. Zachęcam do podjęcia się sklejenia lub wydziergania płaszczyzny hiperbolicznej – konieczne instrukcje znajdzie Czytelnik w artykułach Eryka Kopczyńskiego i Doroty Celińskiej-Kopczyńskiej, opublikowanych w Δ^5_{20}. Jako że funkcja sinh ma wzrost wykładniczy, efekt takiego przedsięwzięcia jest jeszcze bardziej spektakularny niż dla niby-stożka (zob. ilustracje poniżej).

Sałata – proces jej wzrostu przypomina efekt szydełkowania opisany w Δ^5_{20}

Portret Haesje Jacobsdr van Cleyburg, żony pewnego rotterdamskiego piwowara. Rembrandt van Rijn, 1634 (zbiory Rijksmuseum w Amsterdamie)

Przykłady powierzchni o stałej krzywiźnie:
- $\mathbf{0}$: $h(s) = s$, płaszczyzna,
- $\mathbf{R^{-2}}$: $h(s) = R\sin(s/R)$, sfera o promieniu R,
- $\mathbf{-R^{-2}}$: $h(s) = R\sinh(s/R)$, przeskalowana płaszczyzna hiperboliczna.

Powyższe funkcje h łączy to, że spełniają równanie różniczkowe $h'' + k \cdot h = 0$ z warunkami początkowymi $h(0) = 0$, $h'(0) = 1$ (choć dla różnych wartości k). Każdą inną powierzchnię o stałej krzywiźnie da się „zbudować" z jednej z powyższych.

Płaszczyznę hiperboliczną odkryli niezależnie János Bolyai (1802–1860) i Nikołaj Iwanowicz Łobaczewski (1792–1856) (więcej w Δ^8_{18}). Choć nie wynika to bezpośrednio z dotychczasowych obserwacji, płaszczyzna hiperboliczna posiada dużo więcej symetrii niż tylko obrót wokół wyróżnionego punktu, stąd też jej nazwa sugerująca identyczną geometrię wokół każdego punktu. W istocie powierzchnia ta ma w każdym punkcie krzywiznę równą -1 i jest to – w odpowiednim sensie – jedyna taka powierzchnia. Jej zobaczenie utrudnia wykazane przez Davida Hilberta (1862–1943) twierdzenie mówiące, że nie tylko nie można jej przedstawić jako powierzchni obrotowej, ale w ogóle nie da się jej izometrycznie zanurzyć (czyli zrealizować bez deformacji) w przestrzeni trójwymiarowej. Dlatego też sięganie po opis wewnętrzny jest przy zwiedzaniu dziwnych nowych światów nie tylko ciekawe, ale i konieczne.