POLITECHNIKA POZNAŃSKA

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI
Instytut Informatyki

Praca dyplomowa licencjacka

SPRZĘTOWY GENERATOR LICZB LOSOWYCH WYKORZYSTUJĄCY RZUTY KOSTKĄ

Julia Samp, 151775
Jakub Kędra, 151790
Wojciech Kot, 151879
Jakub Prusak, 151178

Promotor
dr inż. Jędrzej Potoniec

POZNAŃ 2025

Spis treści

Rozdział 1

Wstęp

Wstęp do pracy powinien zawierać następujące elementy:

- krótkie uzasadnienie podjęcia tematu;
- cel pracy (patrz niżej);
- zakres (przedmiotowy, podmiotowy, czasowy) wyjaśniający, w jakim rozmiarze praca będzie realizowana;
- ewentualne hipotezy, które autor zamierza sprawdzić lub udowodnić;
- krótką charakterystykę źródeł, zwłaszcza literaturowych;
- układ pracy (patrz niżej), czyli zwięzłą charakterystykę zawartości poszczególnych rozdziałów;
- ewentualne uwagi dotyczące realizacji tematu pracy np. trudności, które pojawiły się w trakcie realizacji poszczególnych zadań, uwagi dotyczące wykorzystywanego sprzętu, współpraca z firmami zewnętrznymi.

No więc co do tego i tamtego testy kurde ten. lol.
xD
tak.

Rozdział 2

Podstawy teoretyczne

Rozdział teoretyczny — przegląd literatury naświetlający stan wiedzy na dany temat.

Przegląd literatury naświetlający stan wiedzy na dany temat obejmuje rozdziały pisane na podstawie literatury, której wykaz zamieszczany jest w części pracy pt. *Literatura* (lub inaczej *Bibliografia*, *Piśmiennictwo*). W tekście pracy muszą wystąpić odwołania do wszystkich pozycji zamieszczonych w wykazie literatury. **Nie należy odnośników do literatury umieszczać w stopce strony.** Student jest bezwzględnie zobowiązany do wskazywania źródeł pochodzenia informacji przedstawianych w pracy, dotyczy to również rysunków, tabel, fragmentów kodu źródłowego programów itd. Należy także podać adresy stron internetowych w przypadku źródeł pochodzących z Internetu.

Rozdział 3

Fragment teoretyczny

Współczesne systemy kryptograficzne oraz aplikacje wymagają generowania liczb losowych, które muszą charakteryzować się wysoką jakością i odpornością na przewidywalność. Najlepiej spełniają do generatory liczb losowych oparte na fizycznych zjawiskach, zwane TRNG (True Random Number Generator). TRNG są szczególnie istotne w kontekście aplikacji wymagających silnej ochrony danych, takich jak systemy kryptograficzne, podpisy cyfrowe, oraz w generowaniu kluczy szyfrujących.

3.1 Zalety dostępnych rozwiązać TRNG

AAAAAAAAAAA, AAAAAAAAAA AAA AAAAAAAAAAAA

3.2 Wady dostępnych rozwiązań TRNG

Mimo że Generatory Liczb Losowych Oparte na Zjawiskach Fizycznych (TRNG) oferują wysoki poziom bezpieczeństwa i losowości, istnieje kilka istotnych wad i ograniczeń związanych z ich implementacją i użytkowaniem. Wśród głównych problemów, które mogą wpływać na wydajność oraz niezawodność TRNG, wyróżnia się następujące aspekty:

3.2.1 Wydajność i szybkość generowania liczb losowych

Wydajność TRNG jest często niższa niż w przypadku Generujących Liczby Losowe Oparte na Algorytmach (PRNG). Generowanie liczb losowych za pomocą zjawisk fizycznych, takich jak szum termiczny czy fluktuacje kwantowe, może być procesem czasochłonnym, szczególnie w systemach wymagających dużych ilości losowych liczb w krótkim czasie. W wyniku tego, TRNG mogą nie spełniać wymagań wydajnościowych w aplikacjach o dużym zapotrzebowaniu na losowość, takich jak systemy kryptograficzne o bardzo wysokiej częstotliwości operacji.

3.2.2 Koszty implementacji

Urządzenia TRNG, zwłaszcza te oparte na zaawansowanych technologiach, takich jak fotonika kwantowa czy detekcja szumów kwantowych, mogą wiązać się z wysokimi kosztami produkcji oraz utrzymania. Z tego powodu, TRNG są często droższe w porównaniu do bardziej ekonomicznych rozwiązań opartych na algorytmach deterministycznych (PRNG), które wystarczają do wielu zastosowań, gdzie wysoka jakość losowości nie jest kluczowym wymaganiem.

3.2.3 Stabilność i jakość generowanych liczb losowych

Choć TRNG są uznawane za bezpieczne, ich jakość może być wpływana przez różne czynniki zewnętrzne, takie jak temperatura, zakłócenia elektromagnetyczne czy inne zmiany środowiskowe. W wyniku tego, generowane liczby losowe mogą wykazywać pewne niskiej jakości właściwości, co wymaga zastosowania dodatkowych mechanizmów, takich jak procesy post-przetwarzania, aby zapewnić ich odpowiednią losowość. Nawet małe zakłócenia w systemie mogą prowadzić do wzorców, które mogą zostać wykorzystane w atakach kryptograficznych.

3.2.4 Skomplikowana kalibracja i konserwacja

Urządzenia TRNG, szczególnie te, które wykorzystują skomplikowane zjawiska fizyczne, wymagają starannej kalibracji i ciągłego monitorowania, aby zapewnić ich prawidłowe funkcjonowanie. W wielu przypadkach konieczne jest stosowanie systemów nadzoru, które monitorują jakość generowanych liczb losowych w czasie rzeczywistym. Ponadto, wymogi dotyczące utrzymania odpowiednich warunków pracy, takich jak stabilna temperatura czy brak zakłóceń elektromagnetycznych, mogą stanowić dodatkową przeszkodę w ich szerokim zastosowaniu.

3.2.5 Złożoność integracji z istniejącymi systemami

Integracja TRNG z już działającymi systemami, zwłaszcza w kontekście urządzeń wbudowanych lub systemów o dużych wymaganiach obliczeniowych, może wiązać się z wieloma trudnościami. Często konieczne jest dostosowanie sprzętu lub oprogramowania w celu zapewnienia kompatybilności i pełnej funkcjonalności. Dodatkowo, ze względu na fizyczną naturę tych urządzeń, integracja z innymi komponentami może prowadzić do wzrostu kosztów oraz złożoności całego systemu.

3.2.6 Ograniczona dostępność i skalowalność

Choć rynek TRNG rośnie, nadal jest on stosunkowo niszowy w porównaniu do bardziej powszechnych rozwiązań opartych na PRNG. Ograniczona dostępność wyspecjalizowanych urządzeń TRNG, szczególnie tych, które oferują wysoką jakość generowanych liczb losowych, sprawia, że ich wdrożenie jest trudniejsze, zwłaszcza w przypadkach wymagających masowej produkcji. Ponadto, nie wszystkie rozwiązania są skalowalne, co może być problemem w przypadku aplikacji wymagających elastyczności i łatwego dostosowywania wydajności do rosnących potrzeb.

3.2.7 Zagadnienia związane z bezpieczeństwem

Chociaż TRNG zapewniają wyższy poziom bezpieczeństwa niż PRNG, nie są one całkowicie odporne na ataki. Ataki fizyczne, takie jak manipulacje w obrębie urządzenia lub przechwytywanie sygnałów z jego elementów, mogą prowadzić do kompromitacji jakości liczb losowych. Ponadto, w przypadku rozwiązań opartych na technologii chmurowej, takich jak te oferowane przez Cloudflare, istnieje ryzyko ataków związanych z przechwytywaniem lub manipulowaniem danymi w trakcie transmisji, co może wpływać na bezpieczeństwo generowanych liczb losowych.

3.2.8 Podsumowanie wad TRNG

Chociaż TRNG oferują niezrównaną jakość losowości w porównaniu do rozwiązań opartych na algorytmach, posiadają również szereg wad, które mogą ograniczać ich szerokie zastosowanie.

Należy do nich niska wydajność, wysokie koszty implementacji, problemy ze stabilnością generowanych liczb losowych, złożoność integracji z systemami oraz ryzyko związane z bezpieczeństwem. W miarę jak technologia będzie się rozwijać, możliwe jest, że te ograniczenia zostaną przezwyciężone, jednak obecnie stanowią one istotne wyzwanie dla szerokiego przyjęcia TRNG w różnych aplikacjach.

3.3 Podsumowanie dostępnych na rynku TRNG

Rozdział 4

Przegląd komercyjnych rozwiązań TRNG

Współczesne systemy kryptograficzne oraz aplikacje wymagają generowania liczb losowych, które muszą charakteryzować się wysoką jakością i odpornością na przewidywalność. Najlepiej spełniają do generatory liczb losowych oparte na fizycznych zjawiskach, zwane TRNG (True Random Number Generator). TRNG są szczególnie istotne w kontekście aplikacji wymagających silnej ochrony danych, takich jak systemy kryptograficzne, podpisy cyfrowe, oraz w generowaniu kluczy szyfrujących.

4.1 Rozwiązania sprzętowe

Wśród komercyjnych rozwiązań sprzętowych, wiodącymi producentami są firmy takie jak **ID Quantique**, **Microchip Technology** i **Semtech**, które oferują zaawansowane urządzenia bazujące na TRNG. Produkty te zapewniają wysoki poziom bezpieczeństwa i są stosowane w wymagających aplikacjach, takich jak bankowość elektroniczna czy systemy wojskowe.

- **ID Quantique** jest jednym z liderów w dziedzinie generatorów liczb losowych opartych na technologii fotoniki. Firma oferuje urządzenia, które wykorzystują detekcję fotonów w celu generowania liczb losowych. Dzięki temu rozwiązania ID Quantique charakteryzują się bardzo wysoką jakością losowości, a jednocześnie są odporne na ataki związane z analizą i przewidywaniem generowanych liczb.
- **Microchip Technology** w swojej ofercie posiada różne moduły TRNG, w tym układy scalone, które generują liczby losowe na podstawie fluktuacji szumów termicznych. Produkty te znajdują zastosowanie w szerokim zakresie aplikacji, od urządzeń mobilnych po systemy wbudowane.
- **Semtech** natomiast oferuje rozwiązania, które wykorzystują zjawiska losowe zachodzące w obwodach analogowych do generowania liczb losowych. Firma ta jest jednym z głównych dostawców układów TRNG, które znajdują szerokie zastosowanie w urządzeniach IoT oraz w systemach komunikacji bezprzewodowej.

4.2 Generatory TRNG w chmurze

W ostatnich latach pojawiły się także rozwiązania chmurowe, które umożliwiają generowanie liczb losowych w czasie rzeczywistym bez potrzeby posiadania własnego sprzętu. Przykładem takiego rozwiązania jest **Cloudflare** – firma specjalizująca się w dostarczaniu usług związanych z

bezpieczeństwem sieciowym. Na swoim blogu Cloudflare przedstawia zaawansowane metody generowania liczb losowych, które są wykorzystywane w ich systemach. Cloudflare korzysta z technologii opartych na zjawiskach fizycznych, takich jak detekcja fizycznych "bąbli"w lampach lawowych ("Entropy Wall"), nieprzewidywalnego fizycznie trójstopniowego wahadła, rozpadu radioaktywnego Uranu oraz procesów związane z tzw. "chaosem kwantowym". Tego typu rozwiązania pozwalają na szybkie i bezpieczne generowanie liczb losowych w skali globalnej, zapewniając jednocześnie wysoki poziom ochrony przed atakami.

Firma ta oferuje użytkownikom dostęp do generatora liczb losowych w chmurze, który jest wykorzystywany m.in. do tworzenia kluczy kryptograficznych oraz w innych zastosowaniach wymagających silnych zabezpieczeń. Dzięki wykorzystaniu globalnej infrastruktury Cloudflare, generowane liczby losowe są szeroko dostępne i charakteryzują się dużą niezawodnością oraz odpornością na ataki.

4.3 Wady dostępnych rozwiązań TRNG

Mimo że Generatory Liczb Losowych Oparte na Zjawiskach Fizycznych (TRNG) oferują wysoki poziom bezpieczeństwa i losowości, istnieje kilka istotnych wad i ograniczeń związanych z ich implementacją i użytkowaniem. Wśród głównych problemów, które mogą wpływać na wydajność oraz niezawodność TRNG, wyróżnia się następujące aspekty:

4.3.1 Wydajność i szybkość generowania liczb losowych

Wydajność TRNG jest często niższa niż w przypadku Generujących Liczby Losowe Oparte na Algorytmach (PRNG). Generowanie liczb losowych za pomocą zjawisk fizycznych, takich jak szum termiczny czy fluktuacje kwantowe, może być procesem czasochłonnym, szczególnie w systemach wymagających dużych ilości losowych liczb w krótkim czasie. W wyniku tego, TRNG mogą nie spełniać wymagań wydajnościowych w aplikacjach o dużym zapotrzebowaniu na losowość, takich jak systemy kryptograficzne o bardzo wysokiej częstotliwości operacji.

4.3.2 Koszty implementacji

Urządzenia TRNG, zwłaszcza te oparte na zaawansowanych technologiach, takich jak fotonika kwantowa czy detekcja szumów kwantowych, mogą wiązać się z wysokimi kosztami produkcji oraz utrzymania. Z tego powodu, TRNG są często droższe w porównaniu do bardziej ekonomicznych rozwiązań opartych na algorytmach deterministycznych (PRNG), które wystarczają do wielu zastosowań, gdzie wysoka jakość losowości nie jest kluczowym wymaganiem.

4.3.3 Stabilność i jakość generowanych liczb losowych

Choć TRNG są uznawane za bezpieczne, ich jakość może być wpływana przez różne czynniki zewnętrzne, takie jak temperatura, zakłócenia elektromagnetyczne czy inne zmiany środowiskowe. W wyniku tego, generowane liczby losowe mogą wykazywać pewne niskiej jakości właściwości, co wymaga zastosowania dodatkowych mechanizmów, takich jak procesy post-przetwarzania, aby zapewnić ich odpowiednią losowość. Nawet małe zakłócenia w systemie mogą prowadzić do wzorców, które mogą zostać wykorzystane w atakach kryptograficznych.

4.3.4 Skomplikowana kalibracja i konserwacja

Urządzenia TRNG, szczególnie te, które wykorzystują skomplikowane zjawiska fizyczne, wymagają starannej kalibracji i ciągłego monitorowania, aby zapewnić ich prawidłowe funkcjonowanie. W wielu przypadkach konieczne jest stosowanie systemów nadzoru, które monitorują jakość generowanych liczb losowych w czasie rzeczywistym. Ponadto, wymogi dotyczące utrzymania odpowiednich warunków pracy, takich jak stabilna temperatura czy brak zakłóceń elektromagnetycznych, mogą stanowić dodatkową przeszkodę w ich szerokim zastosowaniu.

4.3.5 Złożoność integracji z istniejącymi systemami

Integracja TRNG z już działającymi systemami, zwłaszcza w kontekście urządzeń wbudowanych lub systemów o dużych wymaganiach obliczeniowych, może wiązać się z wieloma trudnościami. Często konieczne jest dostosowanie sprzętu lub oprogramowania w celu zapewnienia kompatybilności i pełnej funkcjonalności. Dodatkowo, ze względu na fizyczną naturę tych urządzeń, integracja z innymi komponentami może prowadzić do wzrostu kosztów oraz złożoności całego systemu.

4.3.6 Ograniczona dostępność i skalowalność

Choć rynek TRNG rośnie, nadal jest on stosunkowo niszowy w porównaniu do bardziej powszechnych rozwiązań opartych na PRNG. Ograniczona dostępność wyspecjalizowanych urządzeń TRNG, szczególnie tych, które oferują wysoką jakość generowanych liczb losowych, sprawia, że ich wdrożenie jest trudniejsze, zwłaszcza w przypadkach wymagających masowej produkcji. Ponadto, nie wszystkie rozwiązania są skalowalne, co może być problemem w przypadku aplikacji wymagających elastyczności i łatwego dostosowywania wydajności do rosnących potrzeb.

4.3.7 Zagadnienia związane z bezpieczeństwem

Chociaż TRNG zapewniają wyższy poziom bezpieczeństwa niż PRNG, nie są one całkowicie odporne na ataki. Ataki fizyczne, takie jak manipulacje w obrębie urządzenia lub przechwytywanie sygnałów z jego elementów, mogą prowadzić do kompromitacji jakości liczb losowych. Ponadto, w przypadku rozwiązań opartych na technologii chmurowej, takich jak te oferowane przez Cloudflare, istnieje ryzyko ataków związanych z przechwytywaniem lub manipulowaniem danymi w trakcie transmisji, co może wpływać na bezpieczeństwo generowanych liczb losowych.

4.3.8 Podsumowanie wad TRNG

Chociaż TRNG oferują niezrównaną jakość losowości w porównaniu do rozwiązań opartych na algorytmach, posiadają również szereg wad, które mogą ograniczać ich szerokie zastosowanie. Należy do nich niska wydajność, wysokie koszty implementacji, problemy ze stabilnością generowanych liczb losowych, złożoność integracji z systemami oraz ryzyko związane z bezpieczeństwem. W miarę jak technologia będzie się rozwijać, możliwe jest, że te ograniczenia zostaną przezwyciężone, jednak obecnie stanowią one istotne wyzwanie dla szerokiego przyjęcia TRNG w różnych aplikacjach.

4.4 Podsumowanie dostępnych na rynku TRNG

Rozdział 5

Rozwinięcie/test

Rozdziały dokumentujące pracę własną studenta: opisujące ideę, sposób lub metodę rozwiązania postawionego problemu oraz rozdziały opisujące techniczną stronę rozwiązania — dokumentacja techniczna, przeprowadzone testy, badania i uzyskane wyniki.

Praca musi zawierać elementy pracy własnej autora adekwatne do jego wiedzy praktycznej uzyskanej w okresie studiów. Za pracę własną autora można uznać np.: stworzenie aplikacji informatycznej lub jej fragmentu, zaproponowanie algorytmu rozwiązania problemu szczegółowego, przedstawienie projektu np. systemu informatycznego lub sieci komputerowej, analizę i ocenę nowych technologii lub rozwiązań informatycznych wykorzystywanych w przedsiębiorstwach, itp.

Autor powinien zadbać o właściwą dokumentację pracy własnej obejmującą specyfikację założeń i sposób realizacji poszczególnych zadań wraz z ich oceną i opisem napotkanych problemów. W przypadku prac o charakterze projektowo-implementacyjnym, ta część pracy jest zastępowana dokumentacją techniczną i użytkową systemu.

W pracy **nie należy zamieszczać całego kodu źródłowego** opracowanych programów. Kod źródłowy napisanych programów, wszelkie oprogramowanie wytworzone i wykorzystane w pracy, wyniki przeprowadzonych eksperymentów powinny być umieszczone np. na płycie CD, stanowiącej dodatek do pracy.

Styl tekstu

Należy[1] stosować formę bezosobową, tj. *w pracy rozważono ....., w ramach pracy zaprojektowano ....*, a nie: *w pracy rozważyłem, w ramach pracy zaprojektowałem.* Odwołania do wcześniejszych fragmentów tekstu powinny mieć następującą postać: „Jak wspomniano wcześniej, ...", „Jak wykazano powyżej ....". Należy unikać długich zdań.

Niedopuszczalne są zwroty używane w języku potocznym. W pracy należy używać terminologii informatycznej, która ma sprecyzowaną treść i znaczenie.

Niedopuszczalne jest pisanie pracy metodą *cut&paste*, bo jest to plagiat i dowód intelektualnej indolencji autora. Dane zagadnienie należy opisać własnymi słowami. Zawsze trzeba powołać się na zewnętrzne źródła.

[1] Uwagi o stylu pochodzą częściowo ze stron prof. Macieja Drozdowskiego [1].

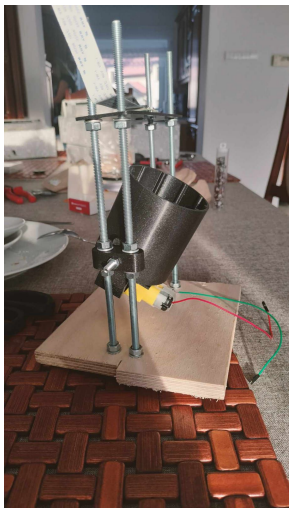
Rozdział 6

Budowa sprzętowego generatora liczb losowych

sectionProjektowanie robota

Proces projektowania robota rozpoczęto od przeanalizowania różnych metod wykonywania rzutu kością. Ostatecznie, po przeanalizowaniu kilku koncepcji, zdecydowano się na rozwiązanie wykorzystujące obrotowy kubek, wewnątrz którego kość porusza się i odbija od ścianek. Taki mechanizm zapewnia losowość rzutu, a jednocześnie jest prosty w konstrukcji i intuicyjny w działaniu. Obracający się kubek został zaprojektowany tak, aby jego prędkość i czas trwania obrotu można było precyzyjnie kontrolować, co w założeniu pozwala na uzyskanie wiarygodnych wyników przy każdym rzucie. W celach testowych został skonstruowany prototypowy model robota, zbudowany w taki sposób, żeby wszystkie jego komponenty były modułowe. Takie rozwiązanie pozwala na łatwą wymianę elementów robota, bez potrzeby przeprojektowywania całego robota od nowa. Przy budowie wykorzystano technologię druku 3D, która pozwala na szybkie modyfikacje przy jednoczesnym zachowaniu bardzo wysokiej dokładności budowy elementów składowych.

Pierwszy prototyp robota składał się z metalowych prętów służących za stelaż oraz elementów wydrukowanych na drukarce 3D. Tymi elementami był: kubek, ramię służące do montażu kubka, uchwyty do prątów oraz płytka mocująca do kamery. Dodatkowo wykorzystano silnik prądu stałego napędzający kubek oraz sterownik służący do zasilania i sterowania ruchem silnika.



Rysunek 6.1: bałagan na stole

Po pierwszych testach okazało się, że niezbędny do uzyskania zamierzonego efektu będzie mechanizm, który będzie wychylał cały kubek wraz z silnikiem, który odpowiada za jego obrót. Z początku planowano wykorzystanie prostogo serwomechanizmu jednak to rozwiązanie odrzucono, ponieważ większość dostępnych serwomechanizmów, które byłyby odpowiednie w tym celu ma ograniczony ruch do 180° lub 360° a to limitowałoby możliwości mechanizmu służącego do wychylania kubka. Ostatecznie w tym celu wybrano mały silnik krokowy z wystarczającym momentem obrotowym (34.3mN.m). Silnik ten obraca układem dwóch kół zębatych 1:2 dzięki czemu silnik ma jeszcze większy zapas momentu obrotowego. Dzięki takiemu rozwiązaniu silnik nie pracuje na granicy swoich możliwości co zapewni jego długi okres eksploatacji.

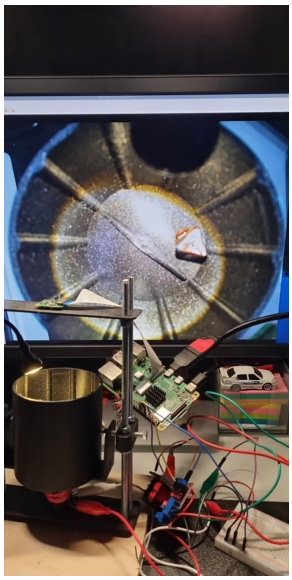
Rysunek 6.2: zebatki

Podczas testów pierwszej wersji robota wykorzytującej obrotowy kubek powstał pomysł alternatywnego rozwiązania. Rozwiązanie to implementuje inne podejście do rzutu kością. Zamiast obracać cały kubek, a dodatkowo wyhylać go, wykorzystany został trwale zamontowany kubek, na którego dnie znajduje się śmigło, które podcina leżącą na dnie kość. Takie rozwiązanie znacząco upraszcza cały mechanizm robota oraz bardzo przyspiesza proces losowania liczby.

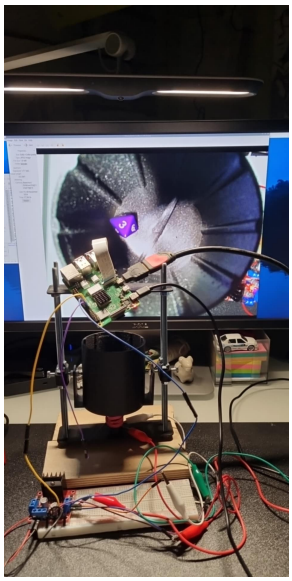
Przy projektowaniu drugiego wariantu robota został wykorzystany ten sam stelaż złożony z metalowych prętów co w pierwszym wariancie. Na drukarce 3D wydrukowano dodatkowe części, niezbędne do realizacji tego wariantu. Zaprojektowano i wydrukowano nowy kubek, śmigło oraz mocowanie dla silnika. Kubek został przystosowany do montażu silnika prądu stałego oraz śmigła.

W obu wariantach dużym problemem był słaby obraz z kamery. W tym celu zaprojektowano system oświetlenia składający się z diod LED, sterowanych za pomocą układu ULN2803A Darlington. Dzięki temu wnętrze kubka stało się dużo jaśniejsze, co pozwala kamerze na robienie zdjęć o wystarczająco dobrej jakości dla zamierzonego celu.

Duże znaczenie ma również wykorzystywana kość. Od jej koloru i tekstury zależy jakość zdjęć zrobionych przez zamonotowaną kamerę. Poniżej przedstawiono dwa przykłady zdjęć i różnic w ich czytelności zależnych od koloru kości.

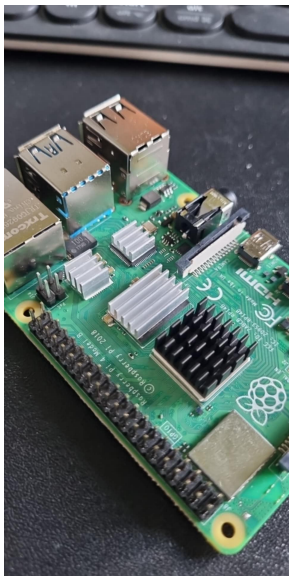


Rysunek 6.3: gorzej



Rysunek 6.4: lepiej

W trakcie testów zauważono, że procesor robota nagrzewa się do wysokich temperatur podczas intensywnej pracy, co mogło negatywnie wpływać na jego wydajność i żywotność. Aby temu zapobiec, w projekcie zdecydowano się na zastosowanie dodatkowych rezystorów, które miały pomóc w rozproszeniu nadmiaru ciepła, oraz wentylatora, który wspomagał cyrkulację powietrza wokół procesora. Dzięki temu rozwiązaniu udało się obniżyć temperaturę pracy procesora, co zapewniło stabilne i bezpieczne działanie całego systemu.



Rysunek 6.5: zimno

6.1 Dokumentacja techniczna

6.1.1 Hardware

aaaaaaaaaaaaaaa

6.1.2 Software

bbbbbbbbbbbbbbbbbbbb

Rozdział 7

Testy

7.1 Użyte testy

Najszerzej stosowanym w świecie narzędziem weryfikacji generatorów (z racji dominowania standardów amerykańskich w dziedzinie ochrony informacji) jest zestaw testów podany przez normę amerykańską FIPS-140-2, dotyczącą bezpieczeństwa modułów kryptograficznych. W badaniu generatorów ciągów bitów losowych norma przewiduje cztery testy istotności. Każdy z nich przeprowadzany jest dla ciągu długości 20000 bitów. [Kotulski, 2001, s. 60]

7.1.1 Test monobitowy

Test monobitowy bada proporcję między liczbą zer a liczbą jedynek w otrzymanym ciągu bitów. Dla wszystkich wygenerowanych bitów zliczono liczbę jedynek w ciągu (X). Nie ma podstaw do odrzucenia ciągu, gdy:

$$9725 < X < 10275$$

7.1.2 Test serii

Celem testu serii jest zliczenie tak zwanych *serii*, czyli nieprzerwanych ciągów takich samych bitów. Test serii sprawdza, czy ilość serii każdej długości jest zgodna z oczekiwanymi wartościami. Test serii bada, czy zmiany między wartościami bitów nie są zbyt częste bądź zbyt rzadkie. Nie ma podstaw do odrzucenia badanego ciągu, gdy:

7.1.3 Test długich serii

Test długich serii polega na sprawdzeniu, czy w testowanym ciągu bitów nie ma zbyt wielu występujących pod rząd takich samych bitów. Ciągi 20 000 bitów nie powinny zawierać serii dłuższych niż 25 bitów.

Długość serii	Przedział
1	2343 - 2657
2	1135 - 1365
3	542 - 708
4	251 - 373
5	111 - 201
6 i więcej	111 - 201

Tabela 7.1: Oczekiwane liczby wystąpień serii

7.1.4 Test pokerowy

Test pokerowy wykorzystuje statystykę chi-kwadrat. Polega na podziale badanego ciągu na segmenty 4-bitowe i zliczeniu liczby wystąpień każdej możliwej z szesnastu kombinacji s_i. Uznaje się, że nie ma podstaw do odrzucenia ciągu, gdy:

$$2,17 < X < 46,17$$

Gdzie:

$$X = \frac{16}{5000} \sum_{i=0}^{15} s_i^2 - 5000$$

7.1.5 Test chi-kwadrat

Aby przeprowadzić ten test, dla wszystkich n rzutów zliczono, ile razy wypadła każda z k ścian kości ośmiościennej (O_i). Wyniki te porównano z oczekiwaną liczbą wyrzucenia każdej ze ścianek $E_i = \frac{n}{k}$. [zdefiniować hipotezę]

$$\chi^2 = \sum_{i=1}^{k} \left(\frac{O_i - E_i}{E_i} \right)^2$$

Ponieważ do generowania liczb losowych użyto kości ośmiościennej, to k jest równe 8, co daje wzór:

$$\chi^2 = \sum_{i=1}^{8} \left(\frac{O_i - E_i}{E_i} \right)^2$$

Poziomem istotności (α) nazywa się prawdopodobieństwo popełnienia błędu pierwszego rzędu. Najczęściej przyjmuje się poziom istotności $\alpha = 0{,}05$. [Koziarska i Metelski, 2016, s. 82] Stopień swobody przy $k = 8$ równa się:

$$k - 1 = 8 - 1 = 7$$

Zatem dla otrzymanego stopnia swobody oraz założonego stopnia istotności, wartość krytyczna wynosi $14,0671$. Jeśli otrzymana wartość będzie mniejsza od wartości krtycznej, nie ma podstaw do odrzucenia hipotezy zerowej.

Rozdział 8

Zakończenie

Zakończenie pracy zwane również Uwagami końcowymi lub Podsumowaniem powinno zawierać ustosunkowanie się autora do zadań wskazanych we wstępie do pracy, a w szczególności do celu i zakresu pracy oraz porównanie ich z faktycznymi wynikami pracy. Podejście takie umożliwia jasne określenie stopnia realizacji założonych celów oraz zwrócenie uwagi na wyniki osiągnięte przez autora w ramach jego samodzielnej pracy.

Integralną częścią pracy są również dodatki, aneksy i załączniki zawierające stworzone w ramach pracy programy, aplikacje i projekty.

Literatura

[1] Maciej Drozdowski. Jak pisać prace dyplomowe – uwagi o formie. [on-line] `http://www.cs.put.poznan.pl/mdrozdowski/dyd/txt/jak_mgr.html`, 2006.

[2] Donald E. Knuth. *The TEXbook*. Computers and Typesetting. Addison-Wesley, Reading, MA, USA, 1986.

[3] Leslie Lamport. *LATEX — A Document Preparation System — User's Guide and Reference Manual*. Addison-Wesley, Reading, MA, USA, 1985.

Dodatek A

Składanie dokumentu w systemie LaTeX

W tym rozdziale znajduje się garść informacji o tym, jak poprawnie składać tekst pracy w systemie LaTeX wraz z przykładami, które mają służyć do przeklejania do własnych dokumentów.

A.1 Struktura dokumentu

Praca składa się z rozdziałów (`chapter`) i podrozdziałów (`section`). Ewentualnie można również rozdziały zagnieżdżać (`subsection`, `subsubsection`), jednak nie powinno się wykraczać poza drugi poziom hierarchii (czyli `subsubsection`).

A.2 Akapity i znaki specjalne

Akapity rozdziela się od siebie przynajmniej jedną pustą linią. Podstawowe instrukcje, które się przydają to *wyróżnienie pewnych słów*. Można również stosować **styl pogrubiony**, choć nie jest to generalnie zalecane.

Należy pamiętać o zasadach polskiej interpunkcji i ortografii. Po spójnikach jednoliterowych warto wstawić znak tyldy (~), który jest tak zwaną „twardą spacją" i powoduje, że wyrazy nią połączone nie będą rozdzielane na dwie linie tekstu.

Polskie znaki interpunkcyjne różnią się nieco od angielskich: to jest „polski", a to jest "angielski". W kodzie źródłowym tego tekstu będzie widać różnicę.

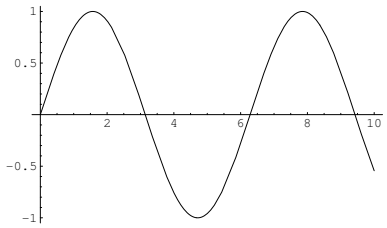
Proszę również zwrócić uwagę na znak myślnika, który może być pauzą „—" lub półpauzą: „–". Należy stosować je konsekwentnie. Do łączenia wyrazów używamy zwykłego „-" (*północno-wschodni*), do myślników — pauzy lub półpauzy. Inne zasady interpunkcji i typografii można znaleźć w słownikach.

A.3 Wypunktowania

Wypunktowanie z cyframi:

1. to jest punkt,
2. i to jest punkt,
3. a to jest ostatni punkt.

Po wypunktowaniach czasem nie warto wstawiać wcięcia akapitowego. Wtedy przydatne jest polecenie `noindent`. Wypunktowanie z kropkami (tzw. *bullet list*) wygląda tak:



Rysunek A.1: Wykres.

- to jest punkt,
- i to jest punkt,
- a to jest ostatni punkt.

Wypunktowania opisowe właściwie niewiele się różnią:

elementA to jest opis,

elementB i to jest opis,

elementC a to jest ostatni opis.

A.4 Polecenia pakietu `ppfcmthesis`

Parę poleceń zostało zdefiniowanych aby uspójnić styl pracy. Są one przedstawione poniżej (oczywiście nie trzeba się do nich stosować).

Makra zdefiniowane dla języka angielskiego. Są nimi: `termdef` oraz `acronym`. Przykłady poniżej obrazują ich przewidywane użycie w tekście.

źródło	`we call this a \termdef{Database Management System} (\acronym{DBMS})`
docelowo	we call this a *Database Management System* (*DBMS*)

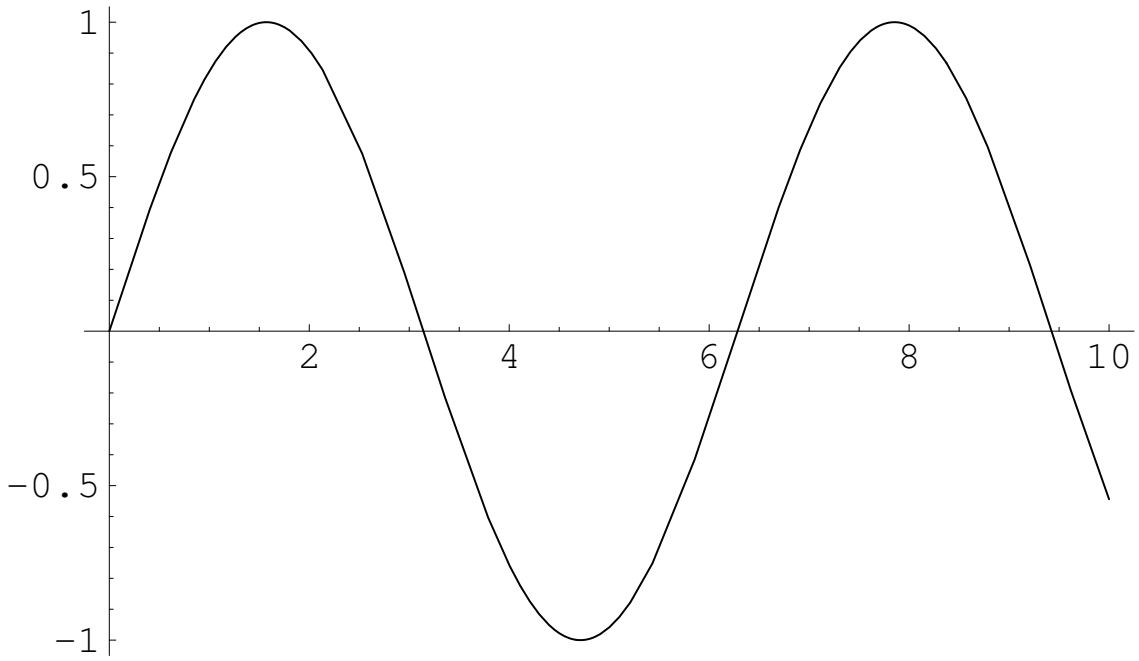
Makra zdefiniowane dla języka polskiego. Podobnie jak dla języka angielskiego zdefiniowano odpowiedniki polskie: `definicja`, `akronim` oraz `english` dla tłumaczeń angielskich terminów. Przykłady poniżej obrazują ich przewidywane użycie w tekście.

źródło	`nazywamy go \definicja{systemem zarządzania bazą danych} (\akronim{DBMS}, \english{Database Management System})`
docelowo	nazywamy go *systemem zarządzania bazą danych* (*DBMS*, ang. *Database Management System*)

A.5 Rysunki

Wszystkie rysunki (w tym również diagramy, szkice i inne) osadzamy w środowisku `figure` i umieszczamy podpis *pod* rysunkiem, w formie elementu `caption`. Rysunki powinny zostać umieszczone u góry strony (osadzone bezpośrednio w treści strony zwykle utrudniają czytanie tekstu). Rysunek A.1 zawiera przykład pełnego osadzenia rysunku na stronie.

Styl FCMu to nieco inne nagłówki rysunków. Dostepne są one poleceniem `fcmfcaption` (zob. rysunek A.2).



Rysunek A.2. Ten sam wykres ale na szerokość tekstu. Formatowanie podpisu zgodne z wytycznymi FCMu.

A.5.1 Tablice

Tablice to piękna rzecz, choć akurat ich umiejętne tworzenie w LaTeXu nie jest łatwe. Jeśli tablica jest skomplikowana, to można ją na przykład wykonać w programie OpenOffice, a następnie wyeksportować jako plik *PDF*. W każdym przypadku tablice wstawia się podobnie jak rysunki, tylko że w środowisko `table`. Tradycja typograficzna sugeruje umieszczenie opisu tablicy, a więc elementu `caption` ponad jej treścią (inaczej niż przy rysunkach).

Tablica A.1 pokazuje pełen przykład.

Tabela A.1: Przykładowa tabela. Styl opisu jest zgodny z rysunkami.

artykuł	cena [zł]
bułka	0, 4
masło	2, 5

Zasady FCMu sugerują nieco inne nagłówki tablic. Dostepne są one poleceniem `fcmtcaption` (zob. tablicę A.2).

Tabela A.2
Przykładowa tabela. Styl opisu jest zgodny z wytycznymi FCMu.

artykuł	cena [zł]
bułka	0, 4
masło	2, 5

A.5.2 Checklista

- Znakiem myślnika jest w LaTeXu dywiz pełen (—) albo półpauza (–), przykład: A niech to jasna cholera — wrzasnąłem.

- Połączenie między wyrazami to zwykły myślnik, przykład: północno-zachodni
- Sprawdź czy tutuł pracy ma maksymalnie dwa wiersze i czy stanowią one pełne frazy (czy nie ma przeniesienia bez sensu).
- Sprawdź ostrzeżenia o 'overfull' i 'underful' boxes. Niektóre z nich można zignorować (spójrz na wynik formatowania), niektóre trzeba poprawić; czasem przeformułować zdanie.

  item Przypisy stawia się wewnątrz zdań lub za kropką, przykład: Footnote is added after a comma.[1]
- Nie używaj przypisów zbyt często. Zobacz, czy nie lepiej będzie zintegrować przypis z tekstem.
- Tytuły tabel, rysunków powinny kończyć się kropką.
- Nie używaj modyfikatora [h] (here) do rysunków i tabel. Rysunki i tabele powinny być justowane do góry strony lub na stronie osobnej.
- Wyróżnienie w tekście to polecenie *wyraz*, nie należy używać czcionki pogrubionej (która wystaje wizualnie z tekstu i rozprasza).
- Nazwy plików, katalogów, ścieżek, zmiennych środowiskowych, klas i metod formatujemy poleceniem `plik_o_pewnej_nazwie`.
- Po ostatniej zmianie do treści, sprawdź i przenieś wiszące spójniki wstawiając przed nie znak tyldy (twardej spacji), przykład: Ala i kotek nie lubią mleczka, a Stasiu lubi.
- Za i.e. (id est) i e.g. (exempli gratia) stawia się zwyczajowo przecinek w typografii amerykańskiej.
- Przed i za pełną pauza nie ma zwyczajowo spacji w typografii amerykańskiej, przykład: Darn, this looks good—said Mary.
- Zamykający cudzysłów oraz footnote wychodzą za ostatni znak interpunkcji w typografii amerykańskiej, przykłady: It can be called a “curiosity,” but it's actually normal. Footnote is added after a comma.[2]
- Odwołania do tabel i rysunków zawsze z wielkiej litery, przykład: In Figure A.1 we illustrated XXX and in Table A.1 we show detailed data.

A.6 Literatura i materiały dodatkowe

Materiałów jest mnóstwo. Oto parę z nich:

- *The Not So Short Introduction...*, która posiada również tłumaczenie w języku polskim.
  `http://www.ctan.org/tex-archive/info/lshort/english/lshort.pdf`
- Klasy stylu `memoir` posiadają bardzo wiele informacji o składzie tekstów anglosaskich oraz sposoby dostosowania LaTeXa do własnych potrzeb.
  `http://www.ctan.org/tex-archive/macros/latex/contrib/memoir/memman.pdf`
- Nasza grupa dyskusyjna i repozytorium Git są również dobrym miejscem aby zapytać (lub sprawdzić czy pytanie nie zostało już zadane).
  `https://github.com/politechnika/put-latex`

[1] Here is a footnote.
[2] Here is a footnote.

- Dla łaknących więcej wiedzy o systemie LaTeX podstawowym źródłem informacji jest książka Lamporta [3]. Prawdziwy *hardcore* to oczywiście *The TEXbook* profesora Knutha [2].

Instytut Informatyki, Wydział Informatyki i Telekomunikacji
Politechnika Poznańska

Skład przy użyciu systemu LaTeX - MiKTeX oraz workflow za pomocą Github Actions.